Elementary number theory

Universität Wuppertal, SS 2018

Jürgen Müller

July 19, 2018

Wenn CD aber AB nicht mißt,
und man nimmt bei AB, CD abwechselnd
immer das kleinere vom größeren weg,
dann muß (schließlich) eine Zahl übrig bleiben,
die die vorangehende mißt.

Eukleídēs — Euklid von Alexandria
'Stoicheia' — Die Elemente, Buch VII, §2.

Contents

1 Introduction: Pythagorean triples

(1.1) Pythagorean triples. We consider the **diophantine** equation $X^2 + Y^2 = Z^2$, that is we look for solutions over the integers $\mathbb{Z}$ [DIOPHANT, ∼250]. To exclude trivialities, we aim at describing the set of all **non-trivial** solutions $[x, y, z] \in \mathbb{Z}^3$ such that $xyz \neq 0$: First, we may of course assume that $x, y, z \in \mathbb{N}$.

Next, if $d := \gcd_+(x, y) \in \mathbb{N}$, then we have $d^2 \mid x^2$ and $d^2 \mid y^2$, hence from $z^2 = x^2 + y^2$ we infer that $d^2 \mid z^2$ as well, implying that $d \mid z$. Thus letting $x' := \frac{x}{d} \in \mathbb{N}$ and $y' := \frac{x}{d} \in \mathbb{N}$ and $z' := \frac{x}{d} \in \mathbb{N}$, we get a **primitive** solution $[x', y', z'] \in \mathbb{N}^3$, that is x' and y' are **coprime** in the sense that $\gcd_+(x', y') = 1$.

Now let $[x, y, z] \in \mathbb{N}^3$ be a primitive solution. Then from x and y being coprime we infer that $\gcd_+(x, z) = \gcd_+(y, z) = 1$ as well.

Assume that x and y are both odd, then there are $r, s \in \{\pm 1\}$ and $k, l \in \mathbb{N}_0$ such that $x = r + 4k$ and $y = s + 4l$. Then we have $z^2 = x^2 + y^2 = r^2 + s^2 + 4(2rk + 2sl + 4k^2 + 4l^2) = 2 + 4m$, for some $m \in \mathbb{N}_0$, saying that z^2 is even, but not divisible by 4. But if $2 \mid z^2$, then $2 \mid z$ as well, hence $4 \mid z^2$, a contradiction.

Thus we infer that exactly one of x and y is even. We may assume that $2 \mid x$. Then from $z^2 = x^2 + y^2$, since x and hence x^2 are even, and y and hence y^2 are odd, we infer that z^2 and hence z are odd. Note that $z > y$.

Thus both $z + y$ and $z - y$ are even, hence $2 \mid \gcd_+(z + y, z - y)$. Moreover, if $d \in \gcd_+(z+y, z-y)$, then $d \mid (z+y)+(z-y) = 2z$ and $d \mid (z+y)-(z-y) = 2y$ imply that $d \mid \gcd_+(2z, 2y) = 2$. Thus we conclude that $\gcd_+(z + y, z - y) = 2$. In other words, we have $\frac{z+y}{2}, \frac{z-y}{2} \in \mathbb{N}$ such that $\gcd_+(\frac{z+y}{2}, \frac{z-y}{2}) = 1$.

We have $\frac{z+y}{2} \cdot \frac{z-y}{2} = \frac{z^2-y^2}{4} = \frac{z^2-y^2}{4} = (\frac{x}{2})^2$, where $\frac{x}{2} \in \mathbb{N}$. Thus from $\frac{z+y}{2}$ and $\frac{z-y}{2}$ being coprime we infer that both $\frac{z+y}{2}$ and $\frac{z-y}{2}$ are squares themselves. Hence there are $a, b \in \mathbb{N}$ such that $a^2 = \frac{z+y}{2}$ and $b^2 = \frac{z-y}{2}$, where we necessarily have $a > b$ and $\gcd_+(a, b) = 1$. This entails $z = \frac{z+y}{2} + \frac{z-y}{2} = a^2 + b^2$ and $y = \frac{z+y}{2} - \frac{z-y}{2} = a^2 - b^2$, and $x^2 = 4 \cdot \frac{z+y}{2} \cdot \frac{z-y}{2} = 4a^2b^2$, implying $x = 2ab$.

Finally, let $r, s \in \{0, 1\}$ and $k, l \in \mathbb{N}_0$ such that $a = r + 2k$ and $b = s + 2l$. Then we have $z = a^2 + b^2 = r^2 + s^2 + 4(rk + sl + k^2 + l^2)$, hence from z being odd we infer that $[r, s] \in \{[0, 1], [1, 0]\}$, that is exactly one of a and b is even. Hence we have shown the major part of the following:

Theorem: [EUCLID]**.** Let $[x, y, z] \in \mathbb{N}^3$ be a primitive solution of $X^2+Y^2 = Z^2$, such that x is even. Then there are uniquely determined $a > b \in \mathbb{N}$ being coprime of opposite parity, such that $x = 2ab$ and $y = a^2 - b^2$ and $z = a^2 + b^2$.

Conversely, any pair $[a, b] \in \mathbb{N}$ having the above properties gives rise to a primitive solution such that x is even. Thus we have a one-to-one correspondence between the primitive solutions as above, and the pairs $[a, b]$ as above.

Proof. We still have to show uniqueness: If $[a, b]$ gives rise to $[x, y, z]$ as above, then we have $a^2 = \frac{z+y}{2}$ and $b^2 = \frac{z-y}{2}$, hence a^2 and b^2, and thus a and b are uniquely determined.

As for the converse, let $a > b \in \mathbb{N}$ be coprime of opposite parity, and let $x := 2ab \in \mathbb{N}$ and $y := a^2 - b^2 \in \mathbb{N}$ and $z := a^2 + b^2 \in \mathbb{N}$. Then we have $z^2 - y^2 = (a^2 + b^2)^2 - (a^2 - b^2)^2 = 4a^2b^2 = x^2$. Moreover, x is even, and since exactly one of a and b is even, we infer that y is odd. Finally, let $d := \gcd_+(x, y) \in \mathbb{N}$. Then we have $d \mid z = a^2 + b^2$, hence from $d \mid y = a^2 - b^2$ we conclude that $d \mid y + z = 2a^2$ and $d \mid y - z = 2b^2$, thus $d \mid \gcd_+(2a^2, 2b^2) = 2$, entailing that $d \in \{1, 2\}$. Now d divides y, which is odd, hence we infer $d = 1$. ♯

In particular, the equation $X^2+Y^2 = Z^2$ has infinitely many non-trivial integral solutions. For example, for $k \in \mathbb{N}$ let $a := k + 1$ and $b := k$. Then the pair $[a, b]$ has the desired properties, and yields the primitive triple $[2ab, a^2-b^2, a^2+b^2] = [2k^2 + 2k, 2k + 1, 2k^2 + 2k + 1]$. In particular, we recover the well-known smallest primitive triples from $k = 1$ and $k = 2$ as $[x, y, z] = [4, 3, 5]$ and $[x, y, z] = [12, 5, 13]$, respectively.

This series of solutions was already known to Pythagoras, who came to study the equation $X^2 + Y^2 = Z^2$ from a geometrical point of view: He was looking for right-angled plane triangles with **commensurable** edges, that is, assuming the longest edge having length 1, the shorter edges have rational length. This essentially amounts to finding right-angled triangles with integral edge lengths, in other words non-trivial integral solutions of the equation $X^2 + Y^2 = Z^2$.

(1.2) Fermat's Last Theorem. Similarly, for any $n \in \mathbb{N}$ we may consider the diophantine equation $X^n + Y^n = Z^n$, and again the aim is to describe the set of all non-trivial solutions $[x, y, z] \in \mathbb{Z}^3$ such that $xyz \neq 0$. Now Fermat [1637] conjectured that the latter do not exist whenever $n \geq 3$. (Actually, he claimed that he had a proof, but unfortunately he kept the proof for himself.) It is immediate that in order to settle Fermat's Conjecture to the affirmative, it suffices to consider the cases $n = 4$ and $n = p$ an odd prime.

From a geometrical point of view, one might ask whether there are right-angled plane triangles with integral edge lengths, such that the shorter ones additionally are squares. This amounts to finding non-trivial integral solutions of the equation $X^4 + Y^4 = Z^2$. It was shown by Euler [1738], that the latter do not exist. In particular, this settles Fermat's Conjecture for the case $n = 4$.

Fermat's Conjecture was proven for the cases $p = 3$ and $p = 5$ by Euler [1753] and Dirichlet, Legendre [1828], respectively. After that it turned out that Fermat's Conjecture was one of the hardest problems in all of number theory. The attempts to solve it spurred lots of developments, starting with the work of Kummer [$\geq$ 1843]. But the final strike was only done by Wiles, Taylor–Wiles [1995], who proved a much more general number theoretic conjecture, which as a consequence settled Fermat's Conjecture for all odd primes p.

I Rings

2 Commutative rings

(2.1) Commutative rings. A set R together with an **addition** $+\colon R \times R \to R\colon [a,b] \mapsto a+b$ and a **multiplication** $\cdot\colon R \times R \to R\colon [a,b] \mapsto ab$ fulfilling the following conditions is called a **commutative ring**: **i)** $(R,+)$ is a commutative group, with neutral element 0; **ii)** $(R,\cdot)$ is a commutative **monoid**, that is commutative and associative, with neutral element 1; and **iii) distributivity** $a(b+c) = (ab)+(ac)$ holds, for $a,b,c, \in R$.

For all $a \in R$ we have $0a = (0+0)a = (0a)+(0a)$, hence $0a = 0$; and we have $a+(-1)a = (1+(-1))a = 0a = 0$, hence $-a = (-1)a$; thus for all $a,b \in R$ we have $-(ab) = (-1)ab = (-a)b$. Moreover, we have the **binomial formula** $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$, for all $n \in \mathbb{N}$.

The standard example of a commutative ring of course are the integers $\mathbb{Z}$; but $\mathbb{N}$ or $\mathbb{N}_0$ are not (commutative) rings. Here is a pathological example:

Let $R := \{0\}$ with addition and multiplication given by $0+0 := 0$ and $0 \cdot 0 := 0$, respectively, and $1 := 0$, then R is a commutative ring, called the **zero ring**. Conversely, for any commutative ring R fulfilling $1 = 0$ we have $a = 1a = 0a = 0$ for all $a \in R$, hence we have $R = \{0\}$. Thus for any commutative ring $R \neq \{0\}$ we in particular have $1 \neq 0$.

(2.2) Units and zero-divisors. a) Let R be a commutative ring. An element $a \in R$ is called **invertible** or a **unit**, if there is an **inverse** $a^{-1} \in R$ such that $aa^{-1} = 1$. In this case, if $a' \in M$ also is an inverse, we have $a' = 1 \cdot a' = a^{-1}aa' = a^{-1} \cdot 1 = a^{-1}$, hence the inverse is uniquely determined.

Let $R^* \subseteq R$ be the set of units. Then we have $1 \in R^*$, where $1^{-1} = 1$; for all $a,b \in R^*$ from $ab(b^{-1}a^{-1}) = 1$ we conclude that $ab \in R^*$, where $(ab)^{-1} = b^{-1}a^{-1}$; and we have $(a^{-1})^{-1} = a$, thus $a^{-1} \in R^*$. Hence $R^* \subseteq R$ is a group, called the **group of multiplicative units**.

Hence for $R \neq \{0\}$ we have $1 \in R^* \subseteq R \setminus \{0\}$. A commutative ring $R \neq \{0\}$ such that $R^* = R \setminus \{0\}$ is called a **field**. Well-known examples are the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$; but we have $\mathbb{Z}^* = \{\pm 1\}$, hence $\mathbb{Z}$ is not a field, of course.

b) An element $a \in R$ is called a **divisor** of $b \in R$, and b is called a **multiple** of a, if there is $c \in R$ such that $ac = b$; we write $a \mid b$. We have $a \mid 0$ and $a \mid a$. Moreover, we have $u \mid a$ for all $u \in R^*$; and if $a \mid u$ for some $u \in R^*$, then we have $a \mid 1$ as well, that is $a \in R^*$. Elements $a,b \in R$ are called **associate**, if $a \mid b$ and $b \mid a$; we write $a \sim b$, in particular $\sim$ is an equivalence relation on R.

An element $0 \neq a \in R$ such that there is $0 \neq b \in R$ such that $ab = 0$ is called a **zero-divisor** in R. If R does not contain any zero-divisors, that is if $ab = 0$ implies $a = 0$ or $b = 0$, for all $a,b \in R$, then R is called an **integral domain**.

For example, $\mathbb{Z}$ is an integral domain, of course.

c) We elucidate the relationship between units and zero-divisors in R:

If $a \in R$ is a unit, then from $ab = 0$, for any $b \in R$, we get $b = a^{-1}ab = 0$, hence a is not a zero-divisor. Hence the set of units and the set of zero-divisors of R are disjoint. In particular, any field is an integral domain.

Lemma. a) For $0 \neq a \in R$ let $\lambda_a \colon R \to R \colon x \mapsto ax$. Then λ_a is injective if and only if a is not a zero-divisor, and λ_a is surjective if and only if a is a unit.

b) Let R be finite. Then any non-zero element of R is either a zero-divisor or a unit. In particular, if R is an integral domain, then R is a field.

Proof. a) If a is a zero-divisor, then there is $0 \neq b \in R$ such that $ab = 0$, thus $ab = 0 = a \cdot 0$ shows that λ_a is not injective. Conversely, if there are $b \neq c \in R$ such that $ab = ac$, then $a \cdot (b - c) = 0$ shows that a is a zero-divisor.

If a is a unit, then for any $b \in R$ we have $a \cdot a^{-1}b = b$, showing that λ_a is surjective. Cconversely, if λ_a is surjective, then there is $b \in R$ such that $ab = 1$, showing that a is a unit.

b) For any $0 \neq a \in R$ the map λ_a is injective if and only if it is surjective. ♯

The disjointness of the set of units and the set of zero-divisors can be rephrased by saying that for $0 \neq a \in R$ the surjectivity of the map λ_a implies its injectivity. The other implication does not hold in general, as the example of $\mathbb{Z}$ shows.

In particular, this shows that for $0 \neq a \in R$ which is not a zero-divisor we have the following **cancellation rule**: From $ab = ac$, for some $b, c \in R$, we get $b = c$. Note that this rule becomes trivial if a is a unit, thus the point here is that it continues to hold under the weaker assumption of a not being a zero-divisor.

(2.3) Ideals. a) Let R be a commutative ring. Then a subset $S \subseteq R$ being an additive subgroup and a multiplicative submonoid is called a **subring**; in particular we have $1 \in S$. For example, $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ is a chain of subrings.

If $\{S_i \subseteq R; i \in \mathcal{I}\}$ is a set of subrings, where $\mathcal{I} \neq \emptyset$ is an index set, then the intersection $S := \bigcap_{i \in \mathcal{I}} S_i \subseteq R$ is a subring again. Hence for any subset $M \subseteq R$ the set $\bigcap\{S \subseteq R \text{ subring}; M \subseteq S\} \subseteq R$ is the smallest subring of R containing M, being called the subring of R **generated** by M.

b) An additive subgroup $I \subseteq R$, such that for all $a \in I$ we have $aR := \{ab \in R; b \in R\} \subseteq I$ as well, is called an **ideal** of R; we write $I \trianglelefteq R$. In particular, we have $\{0\} \trianglelefteq R$ and $R \trianglelefteq R$. Hence for any ideal $I \trianglelefteq R$ we have $I = R$ if and only if $1 \in I$; in particular, I is a subring of R if and only if $I = R$.

If $\{I_i \trianglelefteq R; i \in \mathcal{I}\}$ is a set of ideals, where $\mathcal{I} \neq \emptyset$ is an index set, then the intersection $I := \bigcap_{i \in \mathcal{I}} I_i \trianglelefteq R$ is an ideal again. Hence for any subset $S \subseteq R$ the

set $\langle S\rangle = \langle S\rangle_R := \bigcap\{I \trianglelefteq R; S \subseteq I\} \trianglelefteq R$ is the smallest ideal of R containing S, being called the ideal of R **generated** by S.

More intrinsically, we have $\langle S\rangle = \{\sum_{i=1}^n a_i b_i \in R; n \in \mathbb{N}_0, a_i \in S, b_i \in R\} \trianglelefteq R$; hence we also write $\langle S\rangle = \sum_{a\in S} aR$:

Let $J \subseteq R$ denote the right hand side. If $I \trianglelefteq R$ is any ideal such that $S \subseteq I$, then, since I is closed with respect to addition, and we have $aR \subseteq I$ for all $a \in S$, we have $J \subseteq I$ as well; hence taking intersections we conclude that $J \subseteq \langle S\rangle$. Conversely, J itself is closed with respect to addition, we have $0 \in J$ being represented by the empty sum, and for any $a \in J$ we have $aR \subseteq J$ as well, hence in particular $-a = (-1)\cdot a \in J$; thus $J \trianglelefteq R$ is an ideal, and since $S \subseteq J$ we infer that J is amongst the ideals intersecting in $\langle S\rangle$, thus $\langle S\rangle \subseteq J$. ♯

For any $a \in R$ the ideal $\langle a\rangle = aR \trianglelefteq R$ is called the associated **principal ideal**. Hence for $a, b \in R$ we have $bR \subseteq aR$ if and only if $a \mid b$; in particular we have $aR = bR$ if and only if $a \sim b$. For example, we have $\langle\emptyset\rangle = \langle 0\rangle = 0 \cdot R = \{0\}$ and $\langle 1\rangle = 1 \cdot R = R$; and for $n \in \mathbb{Z}$ we have $\langle n\rangle = n\mathbb{Z} = \{kn \in \mathbb{Z}; k \in \mathbb{Z}\} \trianglelefteq \mathbb{Z}$.

Given $I, J \trianglelefteq R$, then $I + J := \langle I, J\rangle = \{a + b \in R; a \in I, b \in J\} \trianglelefteq R$ is called their **sum**. Moreover, $IJ := \langle ab \in R; a \in I, b \in J\rangle = \{\sum_{i=1}^n a_i b_i \in R; n \in \mathbb{N}_0, a_i \in I, b_i \in J\} \trianglelefteq R$ is called their **product**; we have $IJ \subseteq I \cap J \subseteq I \cup J \subseteq I + J$.

In particular, for principal ideals these constructions yield the following: For $a, b, c \in R$ we have $aR + bR \subseteq cR$ if and only if both $c \mid a$ and $c \mid b$; we have $cR \subseteq aR \cap bR$ if and only if both $a \mid c$ and $b \mid c$; and we have $aR \cdot bR = abR \trianglelefteq R$.

(2.4) Homorphisms. Let R and S be commutative rings. Then a map $\varphi\colon R \to S$ fulfilling the following conditions is called a **(ring) homomorphism**: We have **i) additivity** $\varphi(a + b) = \varphi(a) + \varphi(b)$, for $a, b \in R$; **ii) multiplicativity** $\varphi(ab) = \varphi(a)\varphi(b)$, for $a, b \in R$; and **iii) unitarity** $\varphi(1_R) = 1_S$.

In other words, condition (i) says that φ is a homomorphism of additive groups, and conditions (ii) and (iii) say that φ is a homomorphism of multiplicative monoids. We will see below that, since S is an additivite group, additivity implies $\varphi(0_R) = 0_S$, while multiplicativity alone does not imply unitarity.

If φ is bijective, then it is called a **(ring) isomorphism**, in which case we write $R \cong S$; note that in this case $\varphi^{-1}\colon S \to R$ is a ring isomorphism again.

For example, there is a unique homomorphism $R \to \{0\}$, and there is a (unique) homomorphism $\{0\} \to R$ if and only if $R = \{0\}$.

Proposition. Let $\varphi\colon R \to S$ be a ring homomorphism. Then we have:

a) The image $\mathrm{im}(\varphi) \subseteq S$ is a subring of S

b) The **kernel** $\ker(\varphi) := \varphi^{-1}(\{0\}) = \{a \in R; \varphi(a) = 0\} \trianglelefteq R$ is an ideal of R. Moreover, φ is injective if and only if $\ker(\varphi) = \{0_R\}$.

Proof. a) By additivity $\mathrm{im}(\varphi) \subseteq S$ is closed with respect to addition. We have $\varphi(0_R) = \varphi(0_R + 0_R) = \varphi(0_R) + \varphi(0_R)$, hence $0_S = \varphi(0_R) - \varphi(0_R) = \varphi(0_R) + \varphi(0_R) - \varphi(0_R) = \varphi(0_R)$, showing that $0_S \in \mathrm{im}(\varphi)$. Next we have $0_S = \varphi(0_R) = \varphi(a - a) = \varphi(a) + \varphi(-a)$, hence $\varphi(-a) = -\varphi(a)$, for $a \in R$, thus $\mathrm{im}(\varphi) \subseteq S$ is closed with respect to taking additive inverses. Thus $\mathrm{im}(\varphi) \subseteq S$ is an additive subgroup. Similarly, by multiplicativity $\mathrm{im}(\varphi) \subseteq S$ is closed with respect to multiplication, and we have $1_S \in \mathrm{im}(\varphi)$ by assumption. Hence $\mathrm{im}(\varphi) \subseteq S$ is a multiplicative submonoid as well, and thus is a subring.

b) By additivity $\ker(\varphi) \subseteq R$ is closed with respect to addition. We have $0_R \in \ker(\varphi)$, and $\varphi(-a) = -\varphi(a)$, for $a \in R$, implies that $\ker(\varphi) \subseteq R$ is closed with respect to taking additive inverses. Thus $\ker(\varphi) \subseteq R$ is an additive subgroup. Furthermore, for $x \in \ker(\varphi)$ and $a \in R$ we have $\varphi(xa) = \varphi(x)\varphi(a) = 0_S$, thus $xa \in \ker(\varphi)$. This shows $\ker(\varphi) \cdot R \subseteq \ker(\varphi)$, that is $\ker(\varphi) \trianglelefteq R$ is an ideal.

Moreover, if φ is injective, then $\ker(\varphi) = \varphi^{-1}(\{0_S\})$ is a singleton set, hence necessarily equals $\{0_R\}$; conversely, for $x, y \in R$ we have $\varphi(x) = \varphi(y) \in S$ if and only if $\varphi(x - y) = 0_S$, that is $x - y \in \ker(\varphi)$, thus if $\ker(\varphi) = \{0_R\}$ then $\varphi(x) = \varphi(y)$ entails $x = y$, implying that φ is injective. ♯

Note that if $S \neq \{0\}$, then $\varphi(1_R) = 1_S$ implies that $1_R \notin \ker(\varphi)$, thus $\ker(\varphi) \triangleleft R$.

(2.5) Quotient rings. Let R be a commutative ring, and let $I \trianglelefteq R$ be an ideal. Then $\mathcal{M}_I := \{[a, b] \in R^2; a - b \in I\}$ is an equivalence relation on R:

From $a - a = 0 \in I$, for $a \in R$, we conclude that $\mathcal{M}_I$ is reflexive; from $a - b \in I$, for $a, \in R$, we get $b - a = -(a - b) \in I$, hence $\mathcal{M}_I$ is symmetric; and from $a - b, b - c \in I$, for $a, b, c \in R$, we conclude that $a - c = (a - b) + (b - c) \in I$, thus $\mathcal{M}_I$ is transitive as well. ♯

For $a \in R$ let $\overline{a} = [a]_I := \{b \in R; [a, b] \in \mathcal{M}_I\} = \{b \in R; b - a \in I\} = \{a + x \in R; x \in I\} =: a + I \subseteq R$ be the associated equivalence class **modulo** I. For $a, b \in R$ being in the same equivalence class we also write $a \equiv b \pmod{I}$. Let $R/I := \{a + I \subseteq R; a \in R\}$ denote the set of equivalence classes. This gives rise to the **natural map** $\nu_I \colon R \to R/I \colon a \mapsto a + I$; note that ν_I is surjective.

Letting $R_I \subseteq R$ be a set of **representatives** of R/I, that is the natural map ν_I induces a bijection $R_I \to R/I$, we have $R = \coprod_{a \in R_I} (a + I)$; in other words R is the disjoint union of the distinct equivalence classes. Note that a set of representatives always exists by the Axiom of Choice.

Proposition. Let R be a commutative ring and $I \trianglelefteq R$.

Then R/I is a commutative ring, called the **quotient ring** of R with respect to I, with addition $(a+I)+(b+I) := (a+b)+I$ and multiplication $(a+I)\cdot(b+I) := (ab)+I$, for $a, b \in R$, with additive neutral element $0+I = I$, the additive inverse of $a + I$ being $(-a) + I$, and multiplicative neutral element $1 + I$.

Moreover, the natural map $\nu_I \colon R \to R/I \colon a \mapsto a + I$ is a surjective ring homomorphism such that $\ker(\nu_I) = I$.

Proof. We only have to show that addition and multiplication are independent of the choice of representatives of the equivalence classes; then the rules of arithmetic in R/I are inherited from those in R via the natural map:

Let $a, a', b, b' \in R$ such that $a+I = a'+I$ and $b+I = b'+I$, that is there $x, y \in I$ such that $a' = a + x$ and $b' = b + y$. Hence we have $a' + b' = (a + b) + (x + y) \in (a + b) + I$ and $a'b' = (a + x)(b + y) = ab + (ay + bx + xy) \in ab + I$, thus $(a + b) + I = (a' + b') + I$ and $ab + I = a'b' + I$.

In particular, the natural map becomes a ring homomorphism. Moreover, for $x \in I$ we have $\nu_I(x) = x + I = I = 0 + I \in R/I$, hence $I \subseteq \ker(\nu_I)$; conversely, for $x \in \ker(\nu_I)$ we have $x + I = \nu_I(x) = 0 + I$, hence $x = x - 0 \in I$, showing that $\ker(\nu_I) \subseteq I$. ♯

(2.6) Homomorphism Theorem. Let R and S be commutative rings, let $I \trianglelefteq R$, and let $\varphi\colon R \to S$ be a ring homomorphism such that $I \subseteq \ker(\varphi)$.

Then there is an induced map $\varphi^I\colon R/I \to S\colon a + I \mapsto \varphi(a)$, which is a ring homomorphism and yields a factorisation $\varphi = \varphi^I \circ \nu_I\colon R \to R/I \to S$.

Moreover, we have $\operatorname{im}(\varphi^I) = \operatorname{im}(\varphi) \subseteq S$ and $\ker(\varphi^I) = \ker(\varphi)/I = \{x + I \in R/I; x \in \ker(\varphi)\}$; thus φ^I is injective if and only if $I = \ker(\varphi)$.

In particular, we have a ring isomorphism $\overline{\varphi} := \varphi^{\ker(\varphi)}\colon R/\ker(\varphi) \to \operatorname{im}(\varphi)$.

Proof. We show that φ^I is well-defined: Let $a, a' \in R$ such that $a+I = a'+I$, that is $a - a' \in I \subseteq \ker(\varphi)$, then $\varphi(a - a') = 0$ implies $\varphi(a) = \varphi(a')$.

Now $\varphi^I(a + b + I) = \varphi(a + b) = \varphi(a) + \varphi(b) = \varphi^I(a + I) + \varphi^I(a + I)$ and $\varphi^I(ab + I) = \varphi(ab) = \varphi(a)\varphi(b) = \varphi^I(a + I) \cdot \varphi^I(a + I)$, for $a, b \in R$, and $\varphi^I(1+I) = \varphi(1) = 1$, shows that φ^I is a ring homomorphism. The factorisation holds by construction. Moreover, since ν_I is surjective we infer $\operatorname{im}(\varphi^I) = \operatorname{im}(\varphi)$.

If $x \in \ker(\varphi)$ then $\varphi^I(x + I) = \varphi(x) = 0$, showing that $\ker(\varphi)/I \subseteq \ker(\varphi^I)$; conversely, if $a \in R$ such that $a+I \in \ker(\varphi^I)$, then we have $\varphi(a) = \varphi^I(\nu_I(a)) = \varphi^I(a+I) = 0$, hence $a \in \ker(\varphi)$, and thus $a+I \in \ker(\varphi)/I$, entailing $\ker(\varphi^I) \subseteq \ker(\varphi)/I$. In particular, we have $\ker(\varphi^I) = \{0 + I\}$ if and only if $I = \ker(\varphi)$. This in particular implies the final assertion. ♯

Corollary: Isomorphism Theorem. Let R be a commutative ring and $I \trianglelefteq R$.

a) Let $J \trianglelefteq R$ where $J \subseteq I$. Then we have $(R/J)/(I/J) \cong R/I$.

b) Let $S \subseteq R$ be a subring. Then we have $S/(S \cap I) \cong (S + I)/I$.

Proof. a) We consider the surjective natural map $\nu_I\colon R \to R/I\colon a \mapsto a + I$. Then from $J \subseteq I = \ker(\nu_I)$ we get the existence of a surjective induced map $(\nu_I)^J\colon R/J \to R/I\colon a + J \mapsto a + I$. We have $\ker((\nu_I)^J) = \ker(\nu_I)/J = I/J \trianglelefteq R/J$, hence the induced map $\overline{(\nu_I)^J}\colon (R/J)/(I/J) \to R/I$ is a ring isomorphism.

b) We again consider the natural map $\nu_I\colon R \to R/I\colon a \mapsto a+I$. Then, letting $S+I := \{a+b \in R; a \in S, b \in I\} \subseteq R$, we have $\operatorname{im}(\nu_I|_S) = \nu_I(S) = \{a+I \in R/I; a \in S\} = \{a+I \in R/I; a \in S+I\} = (S+I)/I \subseteq R/I$, and $\ker(\nu_I|_S) = S \cap \ker(\nu_I) = S \cap I \trianglelefteq S$, hence the induced map $\nu_I|_S\colon S/(S\cap I) \to (S+I)/I\colon a+(S\cap I) \mapsto a+I$ is a ring isomorphism. ♯

3 Integral domains

(3.1) Integral domains. a) Let R be an integral domain. We have a characterisation of elements to be associate as follows: Elements $a, b \in R$ are associate, that is $a \mid b$ and $b \mid a$, if and only if there is $u \in R^*$ such that $b = au \in R$:

From $b = au$ for some $u \in R^*$ we have $a \mid b$ and $b \mid a$. Conversely, if $a \mid b$ and $b \mid a$, then there are $u, v \in R$ such that $b = au$ and $a = bv$, thus $a = auv$, implying $a(1-uv) = 0$, hence $a = 0$ or $uv = 1$, where in the first case $a = b = 0$, and in the second case $u, v \in R^*$. ♯

b) Let $\emptyset \neq S \subseteq R$ be a subset. Then $d \in R$ such that $d \mid a$ for all $a \in S$ is called a **common divisor** of S; any $u \in R^*$ always is a common divisor of S. If for all common divisors $b \in R$ of S we have $b \mid d$, then $d \in R$ is called a **greatest common divisor** of S.

Let $\gcd(S) \subseteq R$ be the set of all greatest common divisors of S. In general greatest common divisors do not exist. But if $\gcd(S) \neq \emptyset$, then it consists of an associate class: If $d, d' \in \gcd(S)$, then $d \mid d'$ and $d' \mid d$, hence $d \sim d'$. For $a \in R$ we have $a \in \gcd(a) = \gcd(0, a)$; and elements $a, b \in R$ such that $\gcd(a, b) = R^*$ are called **coprime**.

Similarly, $c \in R$ such that $a \mid c$ for all $a \in S$ is called a **common multiple** of S. If for all common multiples $b \in R$ of S we have $c \mid b$, then $c \in R$ is called a **lowest common multiple** of S.

Let $\operatorname{lcm}(S) \subseteq R$ be the set of all lowest common multiples of S. In general lowest common multiples do not exist. But if $\operatorname{lcm}(S) \neq \emptyset$, then it consists of an associate class: If $c, c' \in \operatorname{lcm}(S)$, then $c \mid c'$ and $c' \mid c$, hence $c \sim c'$. For $a \in R$ we have $a \in \operatorname{lcm}(a) = \operatorname{lcm}(1, a)$.

c) An element $0 \neq c \in R \setminus R^*$ is called **indecomposable** or **irreducible**, if $c = ab$ implies $a \in R^*$ or $b \in R^*$ for all $a, b \in R$; otherwise c is called **decomposable** or **reducible**. Hence if $c \in R$ is indecomposable then all its associates also are.

An element $0 \neq c \in R \setminus R^*$ is called a **prime**, if $c \mid ab$ implies $c \mid a$ or $c \mid b$ for all $a, b \in R$. Hence if $c \in R$ is a prime then all its associates also are.

Lemma. If $c \in R$ is a prime, then $c \in R$ is indecomposable.

Proof. Let $c = ab$ for some $a, b \in R$, where since $c \mid ab$ we may assume that $c \mid a$, then from $a \mid c$ we get $a \sim c$, hence there is $u \in R^*$ such that $au = c = ab$,

implying $b = u \in R^*$. ♯

But the converse does not hold, that is an indecomposable element in general is not a prime. We now introduce a class of integral domains in which the converse indeed holds; it will turn out that $\mathbb{Z}$ belongs to this class:

(3.2) Factorial domains. Let R be an integral domain. Then R is called **factorial** or a **Gaussian domain**, if any element $0 \neq a \in R$ can be written uniquely, up to reordering and taking associates, in the form $a = u \cdot \prod_{i=1}^{n} p_i \in R$, where the $p_i \in R$ are indecomposable, $n \in \mathbb{N}_0$ and $u \in R^*$.

In this case, let $\mathcal{P}_R \subseteq R$ be a set of representatives of the associate classes of indecomposable elements of R; these exist by the Axiom of Choice. Then any $0 \neq a \in R$, up to reordering has a unique **factorisation** $a = u_a \cdot \prod_{p \in \mathcal{P}_R} p^{\nu_p(a)}$, where $u_a \in R^*$ and $\nu_p(a) \in \mathbb{N}_0$ is called the associated **multiplicity**.

We have $\nu_p(a) = 0$ for almost all $p \in \mathcal{P}_R$, and $\sum_{p \in \mathcal{P}_R} \nu_p(a) \in \mathbb{N}_0$ is called the **length** of the factorisation. Moreover, a is called **squarefree** if $\nu_p(a) \leq 1$ for all $p \in \mathcal{P}_R$. For any subset $\emptyset \neq S \subseteq R \setminus \{0\}$ we have $\prod_{p \in \mathcal{P}_R} p^{\min\{\nu_p(a); a \in S\}} \in \gcd(S)$, and provided S is finite we have $\prod_{p \in \mathcal{P}_R} p^{\max\{\nu_p(a); a \in S\}} \in \operatorname{lcm}(S)$. But note that in order to use this in practice, the factorisation of the elements of S has to be found first.

Proposition. Any indecomposable element p of a factorial domain R is a prime.

Proof. Let $a, b \in R$ such that $p \mid ab$, hence there is $c \in R$ such that $pc = ab$. We may assume that $a, b \notin R^*$, and since p is indecomposable we have $c \notin R^*$. Let $a = \prod_{i \geq 1} a_i \in R$ and $b = \prod_{j \geq 1} b_j \in R$ and $c = \prod_{k \geq 1} c_k \in R$, where $a_i, b_j, c_k \in R$ are indecomposable. This yields $p \cdot \prod_{k \geq 1} c_k = \prod_{i \geq 1} a_i \cdot \prod_{j \geq 1} b_j \in R$, thus uniqueness implies $p \sim a_i$ for some i, or $p \sim b_j$ for some j. ♯

(3.3) Euclidean domains. a) An integral domain R is called **Euclidean**, if R has a **degree map** $\delta \colon R \setminus \{0\} \to \mathbb{N}_0$ fulfilling the following condition: **i)** For all $a, b \in R$ such that $b \neq 0$ there are $q, r \in R$, called **quotient** and **remainder** respectively, such that $a = qb + r$, where $r = 0$ or $\delta(r) < \delta(b)$; and **ii)** whenever $a, b \in R$ such that $a \mid b \neq 0$ then we have **monotonicity** $\delta(a) \leq \delta(b)$.

Note that no uniqueness assumption is made in i). Moreover, it actually suffices to require condition i), then condition ii) can fulfilled as well; but in all the cases we will encouter, condition ii) will be automatically fulfilled anyway:

Letting $\delta' \colon R \setminus \{0\} \to \mathbb{N}_0$ obey to condition i), let $\delta \colon R \setminus \{0\} \to \mathbb{N}_0 \colon a \mapsto \min\{\delta'(b) \in \mathbb{N}_0; b \in R \setminus \{0\}, a \mid b\}$. Then δ fulfills condition ii); and for $a, b \in R$ such that $b \neq 0$, letting $0 \neq c \in R$ such that $\delta(b) = \delta'(bc)$, there are $q, r \in R$ such that $a = q(bc) + r = (qc)b + r$, where $r = 0$ or $\delta(r) \leq \delta'(r) < \delta'(bc) = \delta(b)$, implying that condition i) is fulfilled as well. ♯

As a consequence of ii), we have $\delta(a) = \delta(b)$ whenever $a \sim b \neq 0$. Kind of conversely, if $a \mid b \neq 0$ such that $\delta(a) = \delta(b)$, then we have $a \sim b$: Using i), there are $q, r \in R$ such that $a = qb+r$, where $r = 0$ or $\delta(r) < \delta(b)$; but assuming $r \neq 0$ from $a \mid (a - qb) = r$, usinf i) we get $\delta(a) \leq \delta(r) < \delta(b)$, a contradiction; hence we infer $r = 0$, that is $b \mid a$ as well.

For example, any field K is Euclidean with respect to the degree map $\delta\colon K^* \to \mathbb{N}_0\colon x \mapsto 0$. But again our most prominent example is $\mathbb{Z}$, which will turn out to be Euclidean with respect to the degree map $\delta\colon \mathbb{Z} \setminus \{0\} \to \mathbb{N}_0\colon z \mapsto |z|$.

b) The major feature of Euclidean domains is that greatest common divisors always exist, and that they can be computed without factorising:

Given $a, b \in R$, a greatest common divisor $r \in R$ and **Bézout coefficients** $s, t \in R$ such that $r = sa+tb \in R$ can be computed by the **extended Euclidean algorithm (EEA)**; leaving out the steps indicated by $\circ$, needed to compute the $s_i, t_i \in R$, just yields a greatest common divisor:

- $r_0 \leftarrow a$, $r_1 \leftarrow b$
- $\circ$ $s_0 \leftarrow 1$, $s_1 \leftarrow 0$
- $\circ$ $t_0 \leftarrow 0$, $t_1 \leftarrow 1$
- $i \leftarrow 1$
- while $r_i \neq 0$ do
  - $r_{i+1} \leftarrow r_{i-1} \bmod r_i$ # remainder
  - $\circ$ $q_i \leftarrow r_{i-1}$ div r_i # quotient
  - $\circ$ $s_{i+1} \leftarrow s_{i-1} - q_i s_i$
  - $\circ$ $t_{i+1} \leftarrow t_{i-1} - q_i t_i$
  - $i \leftarrow i + 1$
- return $[r; s, t] \leftarrow [r_{i-1}; s_{i-1}, t_{i-1}]$

Since $\delta(r_i) > \delta(r_{i+1}) \geq 0$ for $i \in \mathbb{N}$, there is $l \in \mathbb{N}_0$ such that $r_l \neq 0$ and $r_{l+1} = 0$, hence the algorithm terminates. We have $r_{i+1} = r_{i-1} - q_i r_i$, for all $i \in \{1, \ldots, l\}$, hence $r_i = s_i a + t_i b$ for all $i \in \{0, \ldots, l+1\}$, thus $r = r_l = sa + tb$. Finally, $r = r_l \in \gcd(r_l, 0) = \gcd(r_l, r_{l+1}) = \gcd(r_i, r_{i+1}) = \gcd(r_0, r_1) = \gcd(a, b)$. ♯

(3.4) Theorem: Euclid implies Gauss. Any Euclidean domain is factorial.

Proof. Let R be an Euclidean domain with degree map δ. We first show that any $0 \neq a \in R \setminus R^*$ is a product of indecomposable elements: Assuming the contrary, let a be chosen of minimal degree not having this property. Then a is decomposable, hence there are $b, c \in R \setminus R^*$ such that $a = bc$. Thus by monotonicity we have $\delta(b) < \delta(a)$ and $\delta(c) < \delta(a)$, implying that both b and c are products of indecomposable elements, hence a is a product of indecomposable elements as well, a contradiction.

In order to show uniqueness of factorisations, we next show that any indecomposable element $0 \neq a \in R \setminus R^*$ is a prime: Let $b, c \in R$ such that $a \mid bc$, where may assume that $a \nmid b$. Then we have $1 \in \gcd(a, b)$, hence there are Bézout coefficients $s, t \in R$ such that $1 = sa + tb$, implying that $a \mid sac + tbc = c$.

Now let $a = u \cdot \prod_{i=1}^{n} p_i \in R$, where the p_i are indecomposable, $n \in \mathbb{N}_0$ and $u \in R^*$. We proceed by induction on $n \in \mathbb{N}_0$, where we have $n = 0$ if and only if $a \in R^*$. Hence let $n \geq 1$, and let $a = \prod_{j=1}^{m} q_j \in R$, where the q_j are indecomposable and $m \in \mathbb{N}$. Since p_n is indecomposable, and hence is a prime, we may assume that $p_n \mid q_m$, hence since q_m is indecomposable we infer $p_n \sim q_m$. Thus we have $u' \cdot \prod_{i=1}^{n-1} p_i = \prod_{j=1}^{m-1} q_j \in R$, for some $u' \in R^*$, and we are done by induction. ♯

(3.5) Theorem. Any Euclidean domain is a **principal ideal domain**, that is an integral domain all of whose ideals are principal.

Proof. Let R be Euclidean with degree map δ, and let $I \trianglelefteq R$, where we may assume that $I \neq \{0\}$. Letting $0 \neq x \in I$ be of minimal degree, we show that $I = xR$: We of course have $xR \subseteq I$, hence it remains to show the converse. To this end let $y \in I$. Then there are $q, r \in R$ such that $y = qx + r$, where $r = 0$ or $\delta(r) < \delta(x)$. Hence we have $r = y - qx \in I$, and from the minimality of x we infer that $r = 0$. This shows $y = xq \in xR$, and thus $I \subseteq xR$. ♯

(3.6) Theorem. Any principal ideal domain is factorial. ♯

The converse implication is not true in general, as the example of the polynomial ring $\mathbb{Z}[X]$ shows: By the **Gauss Lemma** (which we do not prove here either), saying that a polyomial ring over a factorial domain is factorial again, $\mathbb{Z}[X]$ is factorial, but the ideal $I := \langle 2, X \rangle \trianglelefteq \mathbb{Z}[X]$ is not principal: Assume that $I = \langle d \rangle$ for some $d \in \mathbb{Z}[X]$, then we have $d \mid 2$ and $d \mid X$, from which, since $1 \in \gcd(2, X)$, we infer $d \mid 1$, entailing $I = \langle 1 \rangle = \mathbb{Z}[X]$; but $\varphi_{\overline{0}} \colon \mathbb{Z}[X] \to \mathbb{Z}/2\mathbb{Z} \colon X \mapsto \overline{0}$ gives rise to a surjective ring homomorphism such that $I \subseteq \ker(\varphi_{\overline{0}})$, hence by the homomorphism theorem we have $\mathbb{Z}[X]/\ker(\varphi_{\overline{0}}) \cong \mathbb{Z}/2\mathbb{Z}$, entailing $I \subseteq \ker(\varphi_{\overline{0}}) \neq \mathbb{Z}[X]$, a contradiction.

In conclusion we have the following inclusions between the various classes of rings we have seen: {fields} $\subset$ {Euclidean domains} $\subset$ {principal ideal domains} $\subset$ {factorial domains} $\subset$ {integral domains} $\subset$ {commutative rings}. The examples presented so far or later on show that all inclusions are proper.

(3.7) Theorem. Let R be a factorial domain, let $a_1, \ldots, a_k \in R \setminus \{0\}$ where $k \in \mathbb{N}$, and let $d \in \gcd(a_1, \ldots, a_k)$ and $c \in \operatorname{lcm}(a_1, \ldots, a_k)$. Then for the associated principal ideals the following holds:

a) We have $\bigcap_{i=1}^{k} a_i R = cR \trianglelefteq R$.

b) If R is a principal ideal domain, then we have $\sum_{i=1}^{k} a_i R = dR \trianglelefteq R$; in particular, there are **Bézout coefficients** $s_1, \ldots, s_k \in R$ such that $d = \sum_{i=1}^{k} a_i s_i \in R$.

c) We have $\bigcap_{i=1}^{k} a_i R = \prod_{i=1}^{k} a_i R \trianglelefteq R$ if and only if the elements $a_1, \ldots, a_k$ are pairwise coprime.

Proof. a) For $x \in R$ we have $x \in \bigcap_{i=1}^k a_i R$ if and only if $a_i \mid x$ for all $i \in \{1, \dots, k\}$, which holds if and only if $c \mid x$, that is $x \in cR$.

b) Since $d \mid a_i$ for all $i \in \{1, \dots, k\}$, we have $\sum_{i=1}^k a_i R \subseteq dR$ anyway. Conversely, since R is a principal ideal domain, there is $d' \in R$ such that $d'R = \sum_{i=1}^k a_i R$. Hence, since $d' \mid a_i$ for all $i \in \{1, \dots, k\}$, we have $d' \mid d$, thus we get $dR \subseteq d'R = \sum_{i=1}^k a_i R$.

c) We have $cR = \bigcap_{i=1}^k a_i R = \prod_{i=1}^k a_i R$ if and only if $c \sim \prod_{i=1}^k a_i$, that is $\prod_{p \in \mathcal{P}_R} p^{\max\{\nu_p(a_i); i \in \{1,\dots,k\}\}} \sim \prod_{p \in \mathcal{P}_R} p^{\sum_{i=1}^k \nu_p(a_i)}$, which holds if and only if $\max\{\nu_p(a_i); i \in \{1, \dots, k\}\} = \sum_{i=1}^k \nu_p(a_i)$, for all $p \in \mathcal{P}_R$, where the latter holds if and only if $\nu_p(a_i) > 0$ for at most one of the a_i, for all $p \in \mathcal{P}_R$, that is the elements $a_1, \dots, a_k$ are pairwise coprime. ♯

II Numbers

4 The integers

The following fundamental theorem was essentially known to Euclid and Legendre [1797], but was first proven by Gauss [1798]. The assertion also follows from (3.4), together with the fact that $\mathbb{Z}$ is Euclidean, see (4.4). Still, following Zermelo [1928], we give a direct proof only using the principle of induction:

(4.1) Theorem: Fundamental Theorem of Arithmetic. $\mathbb{Z}$ is factorial.

Proof. As for the existence of factorisations, we may assume that $n \geq 2$. If n is indecomposable, we are done, in particular settling the case $n = 2$. If n is decomposable, then there are $2 \leq a, b < n$ such that $n = ab$, hence both a and b have a factorisation, thus n has a factorisation as well.

As for uniqueness of factorisations, we assume that $n = \prod_{i=1}^r p_i = \prod_{j=1}^s q_j \in \mathbb{N}$, where $r, s \in \mathbb{N}_0$, and $2 \leq p_1 \leq \cdots \leq p_r$ and $2 \leq q_1 \leq \cdots \leq q_s$ are indecomposable. The case $n = 1$ being clear, we may assume that $n \geq 2$, hence both $r, s \geq 1$. Assume that $p_1 \neq q_1$, where we may assume that $p_1 < q_1$, and let $n' := (q_1 - p_1) \cdot \prod_{j=2}^s q_j = n - p_1 \cdot \prod_{j=2}^s q_j = p_1 \cdot (\prod_{i=2}^r p_i - \prod_{j=2}^s q_j)$. Hence we have $1 \leq n' < n$, and thus by induction n' has a unique factorisation. Since $p_1 \neq q_j$ for all j, hence in particular $p_1 \nmid (q_1 - p_1)$, the left hand side implies that the factorisation of n' does not involve p_1. But the right hand side says that p_1 is involved, a contradiction. Thus we have $p_1 = q_1$, and by cancelling out p_1 we are done by induction. ♯

Since $\mathbb{Z}^* = \{\pm 1\}$, a set of representatives of the associate classes of indecomposable elements is given by the set $\mathcal{P} \subseteq \mathbb{N}$ of positive primes. Thus any $0 \neq z \in \mathbb{Z}$ can be written uniquely as $z = \operatorname{sgn}(z) \cdot \prod_{p \in \mathcal{P}} p^{\nu_p(z)}$, where the **sign** $\operatorname{sgn}(z) \in \{\pm 1\}$ is defined by $\operatorname{sgn}(z) \cdot z > 0$, and $\nu_p(z) \in \mathbb{N}_0$. Thus in particular

Table 1: Euclid-Mullin sequence.

r	$1+\prod_{i=1}^{r-1} p_i$	p_r
1		2
2	3	3
3	7	7
4	43	43
5	1807	13
6	23479	53
7	1244335	5
8	6221671	6221671
9	38709183810571	38709183810571
10	1498400911280533294827535471	139
11	208277726667994127981027430331	2801
12	583385912397051552474857832354331	11
13	641724503636756707723436155897631	17
14	109093165618248640312798414650259711	5471
15	596848709097438311151320126551570873411	52662739

greatest common divisors and lowest common multiples always exist in $\mathbb{Z}$; we write $\gcd_+(\cdot)$ and $\operatorname{lcm}_+(\cdot)$, respectively, for the non-negative ones in question.

(4.2) Theorem: Euclid [~ -300]. $\mathcal{P}$ is infinite.

Proof. Assume to the contrary that $\mathcal{P} = \{p_1, \dots, p_r\}$, for some $r \in \mathbb{N}$, and let $z := 1 + \prod_{i=1}^{r} p_i \in \mathbb{Z}$. Then we have $p_i \nmid z$ for all $i \in \{1, \dots, r\}$, and since z has a factorisation we infer $z = 1$, a contradiction. ♯

Inspired by this, for $z \in \mathbb{Z} \setminus \{0, \pm 1\}$ letting $p_{\min}(z) \in \mathcal{P}$ be the smallest positive prime divisor of z, we consider the **Euclid-Mullin sequence** [Mullin, 1963] recursively defined by $p_1 := 2$ and $p_r := p_{\min}\big(1 + \prod_{i=1}^{r-1} p_i\big) \in \mathcal{P}$, for $r \geq 2$; see Table 1. Hence the Euclid-Mullin sequence consists of pairwise distinct positive primes, thus providing an algorithm to produce infinitely many of them. Noting that typically $1 + \prod_{j=1}^{r-1} p_i$ is not a prime, and that the positive primes do not show up in the Euclid-Mullin in natural order, the question arises whether the Euclid-Mullin sequence contains every positive prime, which is an open problem.

(4.3) Distribution of primes. We wonder how the positive primes are distributed amongst the positive integers. There are various aspects we could possibly consider. We show that in a certain sense there are 'many' primes, that 'locally' primes are not too evenly distributed, but that the 'global' distribution is extremely smooth:

a) For $n \in \mathbb{N}$ let the associated **factorial** be defined as $n! := n \cdot (n-1) \cdots 2 \cdot 1$; we let $0! := 1$. Then for $n \geq 4$ consider $\{n!-n, \ldots, n!-3, n!-2\}$: Since $i \mid (n!-i)$ for all $i \in \{2, \ldots, n\}$, and $n < n! - n$, this set does not contain any prime.

Hence we conclude that amongst the positive integers there are arbitrarily long consecutive gaps without primes. But we also have the following result saying that we indeed have to wait long enough to encouter large gaps:

Theorem: Bertrand's Postulate [1845] [Tchebychef, 1852]**.**
For any $x \geq 1$ the left-open interval $]x, 2x] \subseteq \mathbb{R}$ contains a prime. ♯

b) The following theorem says that compared to all positive integers there are many positive primes, actually many more than squares. To this end, we first recall that the series $\sum_{n\geq 1} \frac{1}{n}$ diverges, while $\sum_{n\geq 1} \frac{1}{n^2}$ exists:

For the former we have the estimate $\sum_{n\geq 1} \frac{1}{n} = 1 + \sum_{k\geq 1} \big(\sum_{n=2^{k-1}+1}^{2^k} \frac{1}{n} \big) \geq 1 + \sum_{k\geq 1} \big(\sum_{n=2^{k-1}+1}^{2^k} \frac{1}{2^k} \big) = 1 + \sum_{k\geq 1} \frac{2^{k-1}}{2^k} = 1 + \sum_{k\geq 1} \frac{1}{2}$, which diverges. For the latter we have $\sum_{n\geq 1} \frac{1}{n^2} \leq 1 + \sum_{n\geq 2} \frac{1}{n(n-1)} = 1 + \sum_{n\geq 2} \big(\frac{1}{n-1} - \frac{1}{n} \big) \leq 2$; actually, we have the surprising result $\sum_{n\geq 1} \frac{1}{n^2} = \frac{\pi^2}{6}$ by Euler [1734]. ♯

Theorem [Euler, 1737]**.** The series $\sum_{p\in\mathcal{P}} \frac{1}{p}$ diverges.

Proof. Assume to the contrary that $\sum_{p\in\mathcal{P}} \frac{1}{p}$ exists. From $\sum_{p\in\mathcal{P}} \big(\frac{1}{p-1} - \frac{1}{p} \big) \leq \sum_{n\geq 2} \big(\frac{1}{n-1} - \frac{1}{n} \big) \leq 1$ we infer that $\sum_{p\in\mathcal{P}} \frac{1}{p-1}$ exists as well. Now, for $n \in \mathbb{N}$ let $\mathcal{P}_{\leq n} := \{p \in \mathcal{P}; p \leq n\}$, and for $z \in \mathbb{Z} \setminus \{0, \pm 1\}$ let $p_{\max}(z) \in \mathcal{P}$ be the largest positive prime divisor of z; let additionally $p_{\max}(\pm 1) := 0$.

Letting $N \in \mathbb{N}$ we have $\sum_{n\leq N} \frac{1}{n} \leq \sum_{p_{\max}(n)\leq N} \frac{1}{n} = \prod_{p\in\mathcal{P}_{\leq N}} \big(\sum_{k\geq 0} p^{-k} \big) = \prod_{p\in\mathcal{P}_{\leq N}} \frac{1}{1-p^{-1}} = \prod_{p\in\mathcal{P}_{\leq N}} \frac{p}{p-1} = \prod_{p\in\mathcal{P}_{\leq N}} \big(1 + \frac{1}{p-1}\big)$.

The natural logarithm $\ln\colon \mathbb{R}_{>0} \to \mathbb{R}$, fulfilling $\frac{\partial}{\partial x} \ln(x) = \frac{1}{x}$ and $\frac{\partial^2}{\partial x^2} \ln(x) = -\frac{1}{x^2}$, is strictly increasing and **concave**, in particular we have $\ln(1+x) \leq x$ for all $x > -1$. Using this we get $\ln\big(\sum_{n\leq N} \frac{1}{n} \big) \leq \ln\big(\prod_{p\in\mathcal{P}_{\leq N}} \big(1 + \frac{1}{p-1}\big) \big) \leq \sum_{p\in\mathcal{P}_{\leq N}} \ln\big(1 + \frac{1}{p-1}\big) \leq \sum_{p\in\mathcal{P}_{\leq N}} \frac{1}{p-1} \leq \sum_{p\in\mathcal{P}} \frac{1}{p-1}$, where by assumption the right hand side exists. Thus $\lim_{N\to\infty} \big(\sum_{n\leq N} \frac{1}{n} \big)$ exists, a contradiction. ♯

c) For $x \in \mathbb{R}_{>0}$ let $\mathcal{P}_{\leq x} := \{p \in \mathcal{P}; p \leq x\}$, and let $\pi(x) := |\mathcal{P}_{\leq x}|$ be the **prime number function**. We are interested in its **asymptotic** behaviour for $x \to \infty$. The following deep theorem was conjectured by Gauss [1793] and Legendre [1798], and first proven by Hadamard, De La Vallée Poussin [1896]:

Prime Number Theorem. We have $\lim_{x\to\infty} \big(\pi(x) \cdot \frac{\ln(x)}{x} \big) = 1$. ♯

The values of $\pi(n)$ and $\lfloor \frac{n}{\ln(n)} \rfloor$, together with $\pi(n) \cdot \frac{\ln(n)}{n}$, where $n := 10^k$ for

Table 2: Prime number function.

$\log_{10}(n)$	$\pi(n)$	$\lfloor \frac{n}{\ln(n)} \rfloor$	$\pi(n) \cdot \frac{\ln(n)}{n}$
1	4	4	0.921034
2	25	21	1.15129
3	168	144	1.1605
4	1229	1085	1.13195
5	9592	8685	1.10432
6	78498	72382	1.08449
7	664579	620420	1.07117
8	5761455	5428681	1.0613
9	50847534	48254942	1.05373
10	455052511	434294481	1.0478

$k \in \{1, \ldots, 10\}$, are given in Table 2. Here, $\lfloor \cdot \rfloor \colon \mathbb{R} \to \mathbb{Z} \colon x \mapsto \max\{z \in \mathbb{Z}; z \leq x\}$ denotes the **(lower) Gauss bracket**. The figures for $\pi(n)$ have been computed using the Sieve of Eratosthenes being described in (4.5).

(4.4) Theorem. $\mathbb{Z}$ is Euclidean with respect to $\delta \colon \mathbb{Z} \setminus \{0\} \to \mathbb{N}_0 \colon z \mapsto |z|$.

Proof. Since δ is monotonous, we only have to show that $\mathbb{Z}$ allows for quotient and remainder with respect to δ. To do so, we even show that for all $a, b \in \mathbb{Z}$ such that $b \neq 0$ there are unique $q, r \in \mathbb{Z}$ such that $a = qb + r$ and $0 \leq r < |b|$:

Let $\mathcal{R} := \{a - xb \in \mathbb{N}_0; x \in \mathbb{Z}, a \geq xb\}$. Since $a + \operatorname{sgn}(b) \cdot |a| \cdot b \in \mathbb{N}_0$ we conclude that $\mathcal{R} \neq \emptyset$. Hence by the Principle of Induction there is a smallest element $r \in \mathcal{R}$, and we let $q \in \mathbb{Z}$ such that $a - qb = r$. Assume that $r \geq |b|$, then we have $a - qb - \operatorname{sgn}(b) \cdot b = r - |b| \geq 0$, contradicting the minimality of r. Hence we have $a = qb + r$ where $0 \leq r < |b|$.

To show uniqueness, let $q', r' \in \mathbb{Z}$ such that $a = q'b + r'$ and $0 \leq r' < |b|$. Then we have $qb + r = a = q'b + r'$, thus $(q - q')b = r' - r$. Hence we have $|q - q'| \cdot |b| = |r' - r| < |b|$, which implies that $q = q'$, and thus $r = r'$ as well. ♯

Using the above notation we denote the **quotient** by $(a \operatorname{div} b) := q \in \mathbb{Z}$, and the **remainder** by $(a \bmod b) := r \in \{0, \ldots, |b| - 1\} =: \mathbb{Z}_{|b|}$, so that we have $a = (a \operatorname{div} b) \cdot b + (a \bmod b)$. Note that for $b > 0$, using the fraction $\frac{a}{b} \in \mathbb{Q}$, we have $(a \operatorname{div} b) = \lfloor \frac{a}{b} \rfloor$.

Thus, since Euclidean domains are factorial, this yields another proof of the Fundamental Theorem of Arithmetic. Moreover, greatest common divisors always in exit in $\mathbb{Z}$, and they can be computed without factorisation, by the extended Euclidean algorithm.

Table 3: Extended Euclidean algorithm in $\mathbb{Z}$.

i	q_i	r_i	s_i	t_i
0		126	1	0
1	3	35	0	1
2	1	21	1	-3
3	1	14	-1	4
4	2	7	2	-7
5		0	-5	18

Example. Letting $a := 2 \cdot 3^2 \cdot 7 = 126$ and $b := 5 \cdot 7 = 35$, Table 3 shows that $r := 7 = 2a - 7b \in \gcd(a, b)$.

(4.5) Computing factorisations. Still we might want to compute factorisations. We turn to the question of how to do this. This is based on the following:

Proposition. Any decomposable $n \in \mathbb{N}$ has a divisor $p \in \mathcal{P}$ where $p \leq \lfloor \sqrt{n} \rfloor$.

Proof. There are $2 \leq a, b < n$ such that $n = ab$, where we may assume that $a \leq \sqrt{n}$. Thus any $p \in \mathcal{P}$ such that $p \mid a$ fulfills $p \leq a \leq \sqrt{n}$ and $p \mid n$. ♯

a) Hence it is useful to determine the set $\mathcal{P}_{\leq n}$ of primes up to some prescribed bound $n \in \mathbb{N}$. This is done using the **Sieve of Eratosthenes** [~ -200]:

- $\mathcal{L} \leftarrow [2, \ldots, n]$
- $k \leftarrow 1$
- while $k \leq \lfloor \sqrt{n} \rfloor$ do
  - if k in $\mathcal{L}$ then # k prime
    - $j \leftarrow k^2$
    - while $j \leq n$ do
      - $\mathcal{L} \leftarrow \mathcal{L} \setminus \{j\}$
      - $j \leftarrow j + k$
  - $k \leftarrow k + 1$
- return $\mathcal{L}$ # contains $\mathcal{P}_{\leq n}$

We may assume that $n \geq 2$, and letting $K := \lfloor \sqrt{n} \rfloor \in \mathbb{N}$ we may even assume that $n = (K+1)^2 - 1 \geq 3$. By induction on k we show that, after $k \in \{1, \ldots, K\}$ has been treated, for $j \in \{2, \ldots, (k+1)^2 - 1\}$ we have $j \in \mathcal{L}$ if and only if j is a prime, and for $j \in \{(k+1)^2, \ldots, n\}$ we have $j \in \mathcal{L}$ if and only if all prime divisors of j exceed k:

For $k = 1$ we have $\mathcal{L} = \{2, 3\} \dot\cup \{4, \ldots, n\}$, hence the assertion holds. Let $k \geq 2$, thus $k < k^2$, and by induction we have $k \in \mathcal{L}$ if and only if k is a prime. If k is not a prime, then $\mathcal{L}$ is unchanged, and for $j \in \{k^2, \ldots, n\}$ we have $j \in \mathcal{L}$ if and only if all prime divisors of j exceed $k - 1$, or equivalently k. If k is a prime,

Table 4: Sieve of Eratosthenes.

	2	**3**	4_2	**5**	6_2	**7**	8_2	9_3	10_2
11	12_2	**13**	14_2	15_3	16_2	**17**	18_2	**19**	20_2
21_3	22_2	**23**	24_2	25_5	26_2	27_3	28_2	**29**	30_2
31	32_2	33_3	34_2	35_5	36_2	**37**	38_2	39_3	40_2
41	42_2	**43**	44_2	45_3	46_2	**47**	48_2	49_7	50_2

---

then $\{k^2, k^2+k, k^2+2k, \ldots\}$ are deleted from $\mathcal{L}$, and then for $j \in \{k^2, \ldots, n\}$ we have $j \in \mathcal{L}$ if and only if $k \nmid j$ and all prime divisors of j exceed $k-1$, which is again equivalent to saying that all prime divisors of j exceed k. In particular, for $j \in \{k^2, \ldots, (k+1)^2-1\}$ we have $j \in \mathcal{L}$ if and only if j is a prime. ♯

In practice, this is run only once for some fixed n, and the set $\mathcal{P}_{\leq n}$ is stored; a typical choice is $n := 10^8$, where $\pi(n) = 5761455$. Note that to save space only the differences between the successive elements of $\mathcal{P}_{\leq n}$ are stored; recall that by Bertrand's Postulate for neighbouring primes $p < q \in \mathcal{P}$ we have $q - p < p$.

Example. This is carried out for $n := 50$, hence $k = 7$, in Table 4: The primes left over are given in bold face, and subscripts indicate at which stage an integer is deleted. Hence we indeed find $\pi(50) = 15$, where

$$\mathcal{P}_{\leq 50} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47\}.$$

b) Given $n \in \mathbb{N}$, let $\mathcal{P}_{\leq \sqrt{n}} = \{p_1, \ldots, p_r\}$, where $r = \pi(\sqrt{n}) \in \mathbb{N}_0$ and $p_1 < \cdots < p_r$. Then the factorisation of n is found by **trial division** as follows:

- $\mathcal{L} \leftarrow []$
- for $p \in [p_1, \ldots, p_r]$ do
  - while $(n \bmod p) = 0$ do
    - $\mathcal{L} \leftarrow \mathcal{L} \sqcup [p]$
    - $n \leftarrow n$ div p
  - if $n = 1$ then
    - return $\mathcal{L}$ # factorisation
- return $[n]$ # n prime

By the Prime Number Theorem, the number of trials needed is given as $\pi(\sqrt{n}) \sim \frac{\sqrt{n}}{\ln(\sqrt{n})} \sim \exp\left(\frac{1}{2}\ln(n) - \ln\ln(n)\right)$. Hence trial division is an **exponential time algorithm**, in terms of the size $\ln(n)$ of the input n. Although there are better integer factorisation algorithms, trial division is used in practice to treat small n, or to discard small prime divisors of large n.

5 Quadratic number rings

(5.1) Quadratic number fields. a) Let $d \in \mathbb{Z} \setminus \{0,1\}$ be squarefree. Let $\sqrt{d} \in \mathbb{R}_{>0} \subseteq \mathbb{C}$ if $d > 0$, and $\sqrt{d} := i \cdot \sqrt{|d|} \in \mathbb{C}$ if $d < 0$, where $i = \sqrt{-1} \in \mathbb{C}$ is the imaginary unit. Let $\mathbb{Q}[\sqrt{d}] := \{a + b\sqrt{d} \in \mathbb{C}; a, b \in \mathbb{Q}\} \subseteq \mathbb{C}$ be the d-th **quadratic number field**, where for $d > 0$ and $d < 0$ the latter is called **real** and **imaginary**, respectively. For $d = -1$ we get the **Gaussian number field** $\mathbb{Q}[i] = \{a + bi \in \mathbb{C}; a, b \in \mathbb{Q}\}$. Note that, if $d' = c^2 d$ for some $0 \neq c \in \mathbb{Z}$, that is d is the **squarefree part** of d', then we have $\mathbb{Q}[\sqrt{d'}] = \mathbb{Q}[\sqrt{d}]$; for $d \in \{0,1\}$ the analogous construction just yields $\mathbb{Q}[\sqrt{0}] = \mathbb{Q}[\sqrt{1}] = \mathbb{Q}$.

From $(a+b\sqrt{d})+(a'+b'\sqrt{d}) = (a+a')+(b+b')\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$ and $c\cdot(a+b\sqrt{d}) = ca + cb\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$, for $a, a', b, b', c \in \mathbb{Q}$, we conclude that $\mathbb{Q}[\sqrt{d}]$ is $\mathbb{Q}$-subspace of $\mathbb{C}$. We show that the $\mathbb{Q}$-generating set $\{1, \sqrt{d}\} \subseteq \mathbb{Q}[\sqrt{d}]$ actually is a $\mathbb{Q}$-basis, in particular we have $\dim_{\mathbb{Q}}(\mathbb{Q}[\sqrt{d}]) = 2$:

Proposition. For $d \in \mathbb{Z} \setminus \{0,1\}$ squarefree, $\{1, \sqrt{d}\}$ is $\mathbb{Q}$-linearly independent.

Proof. Let $a, b \in \mathbb{Q}$ such that $a - b\sqrt{d} = 0 \in \mathbb{C}$, and assume that $[a,b] \neq [0,0]$. Then we have both $a, b \neq 0$. Multiplying both a and b with the product of their denominators, we may assume that $a, b \in \mathbb{Z}$. Hence we get $\sqrt{d} = \frac{a}{b} \in \mathbb{Q}$, in other words $a^2 = b^2 d \in \mathbb{Z}$. This is a contradiction for $d < 0$. Hence we may assume that $d > 0$, in which case we consider factorisations: The multiplicities $\nu_p(a^2) = 2 \cdot \nu_p(a)$ and $\nu_p(b^2) = 2 \cdot \nu_p(b)$ are even, while $\nu_p(d) \in \{0,1\}$, for all $p \in \mathcal{P}$, where there is some $p \in \mathcal{P}$ such that $\nu_p(d) = 1$. Hence all the multiplicities on the left hand side of $a^2 = b^2 d$ are even, while there is an odd one on the right hand side, a contradiction. ♯

From $(a+b\sqrt{d})(a'+b'\sqrt{d}) = (aa'+bb'd)+(ab'+a'b)\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$, for $a, a', b, b' \in \mathbb{Q}$, we conclude that $\mathbb{Q}[\sqrt{d}] \subseteq \mathbb{C}$ is a commutative ring, and since $\mathbb{C}$ is an integral domain, $\mathbb{Q}[\sqrt{d}]$ is so as well. For $0 \neq a + b\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$, that is $[a,b] \neq [0,0]$, we have $(a + b\sqrt{d})^{-1} = \frac{1}{a+b\sqrt{d}} = \frac{a-b\sqrt{d}}{(a+b\sqrt{d})(a-b\sqrt{d})} = \frac{1}{a^2-b^2d} \cdot (a - b\sqrt{d}) \in \mathbb{C}$; note that from $a \pm b\sqrt{d} \neq 0$ we conclude that $a^2 - b^2 d \neq 0$ as well. This shows that $a + b\sqrt{d}$ is a unit in $\mathbb{Q}[\sqrt{d}]$, implying that $\mathbb{Q}[\sqrt{d}]$ indeed is a field.

b) Let $\kappa\colon \mathbb{Q}[\sqrt{d}] \to \mathbb{Q}[\sqrt{d}]\colon a + b\sqrt{d} \mapsto a - b\sqrt{d}$ be the $\mathbb{Q}$-linear **conjugation** map; for $d < 0$ this is just the restriction of **complex conjugation** to $\mathbb{Q}[\sqrt{d}]$.

Then for $a, a', b, b' \in \mathbb{Q}$ we have $\kappa\big((a + b\sqrt{d})(a' + b'\sqrt{d})\big) = \kappa\big((aa' + bb'd) + (ab' + a'b)\sqrt{d}\big) = (aa' + bb'd) - (ab' + a'b)\sqrt{d} = (a - b\sqrt{d}) \cdot (a' - b'\sqrt{d}) = \kappa(a+b\sqrt{d})\cdot\kappa(a'+b'\sqrt{d})$, and we have $\kappa(1) = 1$. Thus κ is a ring isomorphism; for $0 \neq z \in \mathbb{Q}[\sqrt{d}]$ from $\kappa(z)\cdot\kappa(z^{-1}) = \kappa(zz^{-1}) = \kappa(1) = 1$ we get $\kappa(z)^{-1} = \kappa(z^{-1})$.

Now let $N\colon \mathbb{Q}[\sqrt{d}] \to \mathbb{Q}\colon a + b\sqrt{d} \mapsto (a + b\sqrt{d}) \cdot \kappa(a + b\sqrt{d}) = (a + b\sqrt{d}) \cdot (a - b\sqrt{d}) = a^2 - b^2 d$ be the **norm map**. Then we have $N(1) = 1$, and for $z, z' \in \mathbb{Q}[\sqrt{d}]$ we get $N(zz') = N(z)N(z') \in \mathbb{Q}$, hence in particular $N(\kappa(z)) = \kappa(z) \cdot \kappa^2(z) = \kappa(z) \cdot z = N(z)$.

(5.2) Quadratic number rings. a) Let $d \in \mathbb{Z} \setminus \{0,1\}$ be squarefree, and let $\mathbb{Z}[\sqrt{d}] := \{a + b\sqrt{d} \in \mathbb{C}; a, b \in \mathbb{Z}\} \subseteq \mathbb{Q}[\sqrt{d}]$. Then by the above considerations $\mathbb{Z}[\sqrt{d}]$ is a commutative ring, hence is an integral domain, being called a **quadratic number ring**, where for $d > 0$ and $d < 0$ it is called **real** and **imaginary**, respectively; recall that $\{1, \sqrt{d}\}$ is $\mathbb{Q}$-linearly independent. For $d = -1$ we get the **Gaussian integers** $\mathbb{Z}[i] = \{a + bi \in \mathbb{C}; a, b \in \mathbb{Z}\}$ [1807].

In particular, the conjugation map on $\mathbb{Q}[\sqrt{d}]$ restricts to a ring isomorphism $\kappa\colon \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}[\sqrt{d}]\colon a+b\sqrt{d} \mapsto a-b\sqrt{d}$, and similarly the norm map $\mathbb{Q}[\sqrt{d}] \to \mathbb{Q}$ yields a map $N\colon \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}\colon z \mapsto z \cdot \kappa(z)$.

b) If $4 \mid (d-1)$, then let $\mathbb{Z}[\frac{1+\sqrt{d}}{2}] := \{a + b\frac{1+\sqrt{d}}{2} \in \mathbb{C}; a, b \in \mathbb{Z}\} = \{\frac{1}{2}(2a + b + b\sqrt{d}) \in \mathbb{C}; a, b \in \mathbb{Z}\} = \{\frac{1}{2}(a + b\sqrt{d}) \in \mathbb{C}; a, b \in \mathbb{Z},\ 2 \mid (a-b)\} \subseteq \mathbb{Q}[\sqrt{d}]$; note that $\{1, \frac{1+\sqrt{d}}{2}\}$ is $\mathbb{Q}$-linearly independent, and that $\mathbb{Z}[\sqrt{d}] \subset \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. We show that $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ is a commutative ring, also being called a **quadratic number ring**; in particular, for $d = -3$ we get the **Eisenstein integers** $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}] = \{\frac{1}{2}(a + b\sqrt{-3}) \in \mathbb{C}; a, b \in \mathbb{Z},\ 2 \mid (a-b)\}$:

For $a, a', b, b' \in \mathbb{Z}$ such that $2 \mid (a-b)$ and $2 \mid (a'-b')$, we get $\frac{1}{2}(a + b\sqrt{d}) \cdot \frac{1}{2}(a' + b'\sqrt{d}) = \frac{1}{2}\big(\frac{aa'+bb'd}{2} + \frac{ab'+a'b}{2} \cdot \sqrt{d}\big)$. Writing $d = 4k+1$ for some $k \in \mathbb{Z}$, in particular saying that d is odd, and noting that both $\{a, b\}$ and $\{a', b'\}$ are either both even or both odd, we conclude that both $aa' + bb'd$ and $ab' + a'b$ are even, and that $aa' + bb'd - (ab' + a'b) = 4kbb' + aa' + bb' - ab' - a'b = 4kbb'+(a-b)(a'-b')$ is divisible by 4, implying that $\frac{aa'+bb'd}{2} \in \mathbb{Z}$ and $\frac{ab'+a'b}{2} \in \mathbb{Z}$ such that $2 \mid (\frac{aa'+bb'd}{2} - \frac{ab'+a'b}{2})$. ♯

Hence we get the ring isomorphism $\kappa\colon \mathbb{Z}[\frac{1+\sqrt{d}}{2}] \to \mathbb{Z}[\frac{1+\sqrt{d}}{2}]\colon \frac{1}{2}(a + b\sqrt{d}) \mapsto \frac{1}{2}(a-b\sqrt{d})$, where $a, b \in \mathbb{Z}$ such that $2 \mid (a-b)$; note that $2 \mid (a-b+2b) = (a+b)$.

Moreover, for $a, b \in \mathbb{Z}$ such that $2 \mid (a-b)$, writing $a = \alpha + 2l$ and $b = \beta + 2m$, where either $\alpha = \beta = 1$ or $\alpha = \beta = 0$, and $l, m \in \mathbb{Z}$, we get $a^2 - b^2d = \alpha^2 + 4l(\alpha+l) - (\beta^2 + 4m(\beta+m))(1+4k) = \alpha^2 - \beta^2 + 4n = 4n$, for some $n \in \mathbb{Z}$. Hence we indeed get a norm map $N\colon \mathbb{Z}[\frac{1+\sqrt{d}}{2}] \to \mathbb{Z}\colon \frac{1}{2}(a+b\sqrt{d}) \mapsto \frac{1}{4}(a^2 - b^2d)$.

(5.3) Units in quadratic number rings. We aim at describing the units in quadratic number rings, which never are fields, and where it turns out that the real and imaginary cases behave fundamentally differently.

Theorem. Let $d \in \mathbb{Z} \setminus \{0,1\}$ be squarefree.

a) We have $\mathbb{Z}[\sqrt{d}]^* = \{z \in \mathbb{Z}[\sqrt{d}]; |N(z)| = 1\}$.

If $4 \mid (d-1)$ then similarly we have $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]^* = \{z \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]; |N(z)| = 1\}$.

b) For $d < 0$ we get the following: For $d \leq -2$ we get $\mathbb{Z}[\sqrt{d}]^* = \{\pm 1\}$, while for $d = -1$ we have $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$; note that $\mathbb{Z}[i]^* = \{1, i, i^2, i^3\}$.

If $4 \mid (d-1)$ then similarly for $d \le -7$ we get $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]^* = \{\pm 1\}$, while for $d \le -3$ we have $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]^* = \{\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}\}$; note that letting $\zeta_6 := \frac{1+\sqrt{-3}}{2} \in \mathbb{C}$ we have $\zeta_6^2 = \frac{-1+\sqrt{-3}}{2}$ and $\zeta_6^3 = -1$, hence $\mathbb{Z}[\zeta_6]^* = \{1, \zeta_6, \zeta_6^2, \dots, \zeta_6^5\}$.

Proof. a) Since $N\colon \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}$ is multiplicative such that $N(1) = 1$, we conclude that N restricts to a group homomorphism $N\colon \mathbb{Z}[\sqrt{d}]^* \to \mathbb{Z}^* = \{\pm 1\}$, implying $\mathbb{Z}[\sqrt{d}]^* \subseteq \{z \in \mathbb{Z}[\sqrt{d}]; |N(z)| = 1\}$; conversely, if $z \in \mathbb{Z}[\sqrt{d}]$ such that $N(z) = z \cdot \kappa(z) \in \{\pm 1\}$, then $z^{-1} = N(z) \cdot \kappa(z) \in \mathbb{Z}[\sqrt{d}]$, hence $z \in \mathbb{Z}[\sqrt{d}]^*$.

Similarly, if $4 \mid (d-1)$ the group homomorphism $N\colon \mathbb{Z}[\frac{1+\sqrt{d}}{2}]^* \to \mathbb{Z}^*$ implies $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]^* \subseteq \{z \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]; |N(z)| = 1\}$; conversely, if $z \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ such that $N(z) = z \cdot \kappa(z) \in \{\pm 1\}$, then $z^{-1} = N(z) \cdot \kappa(z) \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$, hence $z \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]^*$.

b) For $d < 0$ we get $\mathbb{Z}[\sqrt{d}]^* = \{a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]; a^2 + b^2 \cdot |d| = 1\}$, in particular for $d = -1$ we have $\mathbb{Z}[i]^* = \{a + bi \in \mathbb{Z}[i]; a^2 + b^2 = 1\}$; this implies the assertion.

Similarly, if $4 \mid (d-1)$ then we get $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]^* = \{\frac{1}{2}(a + b\sqrt{d}) \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]; a^2 + b^2 \cdot |d| = 4\}$, in particular for $d = -3$ we have $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]^* = \{\frac{1}{2}(a + b\sqrt{-3}) \in \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]; a^2 + 3b^2 = 4\}$; this implies the assertion. ♯

Theorem. Let $d \ge 2$ be squarefree. Then the (multiplicative) group of units $\mathbb{Z}[\sqrt{d}]^* = \{a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]; a^2 - b^2 d \in \{\pm 1\}\}$ is infinite of shape $\{\pm 1\} \times \langle \epsilon_d \rangle$.

If $4 \mid (d-1)$ then similarly $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]^* = \{\frac{1}{2}(a + b\sqrt{d}) \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]; a^2 - b^2 d \in \{\pm 4\}\}$ is infinite of shape $\{\pm 1\} \times \langle \epsilon'_d \rangle$; here ϵ_d and ϵ'_d are called **fundamental** units. ♯

(5.4) Quadratic number rings as factorial domains. Let $d \in \mathbb{Z} \setminus \{0, 1\}$ be squarefree, and to unify notation let $\mathcal{O}_d := \mathbb{Z}[\sqrt{d}]$ if $4 \nmid (d-1)$, and $\mathcal{O}_d := \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ if $4 \mid (d-1)$; that is (for reasons we are not explaining here) in the latter case we consider the larger of the quadratic number rings.

We wonder which $\mathcal{O}_d$ are factorial, where again we distinguish the cases $d < 0$ and $d > 0$. For $d < 0$, the following deep theorem was conjectured by Gauss [1798] and first proven by Stark [1967]:

Theorem. Let $d < 0$. Then $\mathcal{O}_d$ is factorial if and only if

$$d \in \{-1, -2\} \,\dot\cup\, \{-3, -7, -11\} \,\dot\cup\, \{-19, -43, -67, -163\},$$

where the first bunch are the values such that $4 \nmid (d-1)$, while the latter two bunches are the values such that $4 \mid (d-1)$, and the first two bunches by (5.6) are the values for which $\mathcal{O}_d$ is Euclidean. ♯

In contrast, for $d > 0$ it still is an open problem which rings $\mathcal{O}_d$ are factorial, where it is even unknown whether infinitely many of them are so. For $d \le 30$ the ring $\mathcal{O}_d$ is factorial if and only if $d \in \{2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 22, 23, 29\}$,

of which by (5.6) only for $d \in \{14, 22, 23\}$ the ring $\mathcal{O}_d$ is not Euclidean with respect to the norm map.

Example. i) We look for specific elements being indecomposable, but not a prime [DEDEKIND, 1871]: To this end, let $d \leq -3$ be odd, and we consider the ring $\mathbb{Z}[\sqrt{d}]$, for which we have $\mathbb{Z}[\sqrt{d}]^* = \{\pm 1\}$. From $N(a+b\sqrt{d}) = a^2+b^2 \cdot |d| \geq 0$, for $a, b \in \mathbb{Z}$, we conclude $N(a + b\sqrt{d}) \neq 2$.

We show that $2 \in \mathbb{Z}[\sqrt{d}]$ is indecomposable, but not a prime: Assume that $2 = xy$, where $x, y \in \mathbb{Z}[\sqrt{d}] \setminus \{\pm 1\}$, hence we have $N(x)N(y) = N(xy) = N(2) = 4$, and since $N(x), N(y) > 1$ we conclude $N(x) = N(y) = 2$, a contradiction. Moreover, we have $2 \mid 1 + |d| = (1 + \sqrt{d})(1 - \sqrt{d}) \in \mathbb{Z}[\sqrt{d}]$, but a comparison of coefficients shows $2 \nmid (1 \pm \sqrt{d})$.

Hence we conclude that $\mathbb{Z}[\sqrt{d}]$ is not factorial. This proves the above theorem for $4 \mid (d + 1)$. As there are $d \leq -3$ such that $4 \mid (d - 1)$ and $\mathcal{O}_d$ is factorial, we observe that $\mathbb{Z}[\sqrt{d}]$ and $\mathcal{O}_d$ indeed might be essentially different.

ii) Let $d \leq -5$ be odd such that $4 \mid (d + 1)$. We show that $d - 1$ and $2 + 2\sqrt{d}$ do not have a greatest common divisor in $\mathbb{Z}[\sqrt{d}]$:

Assume $z = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, where $a, b \in \mathbb{Z}$, is a greatest common divisor. Then taking norms we get $N(z) \mid (d - 1)^2$ and $N(z) \mid 4(d - 1)$, hence $N(z) \mid (d-1) \cdot \gcd_+(4, d-1)$. Moreover, $2 \mid z \in \mathbb{Z}[\sqrt{d}]$ yields $4 \mid N(z)$, and $(1+\sqrt{d}) \mid z \in \mathbb{Z}[\sqrt{d}]$ yields $(d - 1) \mid N(z)$, thus $\frac{4(d-1)}{\gcd_+(4,d-1)} \mid N(z)$. Hence we conclude that $\frac{4}{\gcd_+(4,d-1)} \cdot (d - 1) \mid N(z) \mid (d - 1) \cdot \gcd_+(4, d - 1)$. Since $4 \mid (d + 1)$ we have $\gcd_+(4, d - 1) = 2$, and thus $a^2 + b^2 \cdot |d| = N(z) = 2(1 - d)$. Hence we get $b \in \{0, \pm 1\}$. If $b = 0$, then a comparison of coefficients yields $z = a \in \{\pm 1, \pm 2\}$, hence $N(z) \in \{1, 4\}$, a contradiction. If $|b| = 1$, then we get $a^2 = 2 - d$, hence a is odd, thus $4 \mid (a + 1)(a - 1) = a^2 - 1 = d - 1$, a contradiction. ♯

iii) For $-12 \leq d < -2$ even, there are just two cases to be considered:

For $d := -6$ we get $2 \cdot 3 = (\sqrt{-6}) \cdot (-\sqrt{-6}) \in \mathbb{Z}[\sqrt{-6}]$. From $N(a + b\sqrt{-6}) = a^2 + 6b^2 \geq 0$, for $a, b \in \mathbb{Z}$, we infer that $N(z) \notin \{2, 3\}$ for all $z \in \mathbb{Z}[\sqrt{-6}]$. Hence $N(2) = 4$ and $N(3) = 9$ and $N(\pm\sqrt{-6}) = 6$ imply that these elements are all indecomposable, while the above product says that none of them is a prime. Hence $\mathbb{Z}[\sqrt{-6}]$ is not factorial.

For $d := -10$ we get $2 \cdot 5 = (\sqrt{-10}) \cdot (-\sqrt{-10}) \in \mathbb{Z}[\sqrt{-10}]$. From $N(a + b\sqrt{-10}) = a^2 + 10b^2 \geq 0$, for $a, b \in \mathbb{Z}$, we infer that $N(z) \notin \{2, 5\}$ for all $z \in \mathbb{Z}[\sqrt{-10}]$. Hence $N(2) = 4$ and $N(5) = 25$ and $N(\pm\sqrt{-10}) = 10$ imply that these elements are all indecomposable, while the above product says that none of them is a prime. Hence $\mathbb{Z}[\sqrt{-10}]$ is not factorial.

(5.5) Quadratic number rings as principal ideal domains. This is immediately settled; recall that principal ideal domains are factorial anyway:

Theorem. Let $d \in \mathbb{Z} \setminus \{0,1\}$ be squarefree. Then the ring $\mathcal{O}_d$ is a principal ideal domain if and only if it is factorial. ♯

Example. We consider the ring $R := \mathbb{Z}[\sqrt{-5}]$, which is not factorial, and hence possesses non-principal ideals. Indeed these are related to non-unique factorisations, which can be unified using ideals of R:

We have $R^* = \{\pm 1\}$ and $N(a + b\sqrt{-5}) = a^2 + 5b^2$; in particular we have $N(a + b\sqrt{-5}) \notin \{2, 3\}$. Thus $N(2) = 4$ and $N(3) = 9$ and $N(1 \pm \sqrt{-5}) = 6$ show that the elements $2, 3, 1 \pm \sqrt{-5} \in R$ are indecomposable. Hence $2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ are two essentially different factorisations.

Let $I_2 := \langle 2, 1 + \sqrt{-5}\rangle$ and $I_3^\pm := \langle 3, 1 \pm \sqrt{-5}\rangle$. Then we have $I_2^2 = \langle 4, 2 + 2\sqrt{-5}, -4 + 2\sqrt{-5}\rangle = \langle 2\rangle$ and $I_3^+ I_3^- = \langle 9, 3 + 3\sqrt{-5}, 3 - 3\sqrt{-5}, 6\rangle = \langle 3\rangle$, as well as $I_2 I_3^+ := \langle 6, 2 + 2\sqrt{-5}, 3 + 3\sqrt{-5}, -4 + 2\sqrt{-5}\rangle = \langle 1 + \sqrt{-5}\rangle$ and $I_2 I_3^- := \langle 6, 2 - 2\sqrt{-5}, 3 + 3\sqrt{-5}, 6\rangle = \langle 1 - \sqrt{-5}\rangle$. Thus we get $I_2^2 \cdot I_3^+ I_3^- = \langle 2\rangle\langle 3\rangle = \langle 6\rangle = \langle 1 + \sqrt{-5}\rangle\langle 1 - \sqrt{-5}\rangle = I_2 I_3^+ \cdot I_2 I_3^-$, showing that both factorisations lead to the same product of ideals.

We determine $|R/I_2|$ and $|R/I_3^\pm|$: For $a + b\sqrt{-5} \in R$ we have $a + b\sqrt{-5} \equiv a - b \equiv ((a - b) \bmod 2) \pmod{I_2}$, implying that $|R/I_2| \leq 2$; since $I_2^2 = \langle 2\rangle \neq R$ implies $I_2 \neq R$ as well, we deduce $|R/I_2| = 2$. Similarly, we have $a + b\sqrt{-5} \equiv a \mp b \equiv ((a \mp b) \bmod 3) \pmod{I_3^\pm}$, implying that $|R/I_3^\pm| \leq 3$; since $I_3^+ I_3^- = \langle 3\rangle \neq I_3^\pm$ we have $I_3^\pm \neq R$; assuming that $1 \equiv -1 \pmod{I_3^\pm}$ yields $2 \in I_3^\pm$, hence $1 = 3 - 2 \in I_3^\pm$, a contradiction; we deduce $|R/I_3^\pm| = 3$.

We show I_2 and $I_3^\pm$ are non-principal ideals: Assume that $I_2 = \langle z\rangle$ for some $z \in R$; then $z \mid 2$ and $z \mid 1 + \sqrt{-5}$, entailing $N(z) \mid N(2) = 4$ and $N(z) \mid N(1 + \sqrt{-5}) = 6$, hence $N(z) \mid 2$, and thus $N(z) = 1$, that is $z \in \{\pm 1\}$, and hence $I_2 = R$, a contradiction. Similarly, assume that $I_3^\pm = \langle z\rangle$ for some $z \in R$; then $z \mid 3$ and $z \mid 1 \pm \sqrt{-5}$, entailing $N(z) \mid N(3) = 9$ and $N(z) \mid N(1 \pm \sqrt{-5}) = 6$, hence $N(z) \mid 3$, that is $z \in \{\pm 1\}$, and hence $I_3^\pm = R$, a contradiction.

Since the elements $2, 3, 1 \pm \sqrt{-5} \in R$ are indecomposable and non-associate, we infer these elements are pairwise coprime, that is we may let $d_2 := 1 \in \gcd(2, 1 + \sqrt{-5})$ and $d_3^\pm := 1 \in \gcd(3, 1 \pm \sqrt{-5})$. But we have $I_2 \subset \langle d_2\rangle = R$ and $I_3^\pm \subset \langle d_3^\pm\rangle = R$, saying that the greatest common divisors in question cannot be written as a sum of multiples of the elements under consideration. ♯

(5.6) Quadratic number rings as Euclidean domains. Let $d \in \mathbb{Z} \setminus \{0,1\}$ be squarefree. We wonder which $\mathcal{O}_d$ are Euclidean. This is rarely the case:

Theorem. The ring $\mathcal{O}_d$ is Euclidean with respect to the norm map, that is has degree map $\delta\colon \mathcal{O}_d \setminus \{0\} \to \mathbb{N}_0\colon z \mapsto |N(z)|$, if (but not only if)

$$d \in \{-1, -2\} \dot\cup \{-3, -7, -11\} \dot\cup \{2, 3\} \dot\cup \{5, 13\},$$

where we distinguish the cases $4 \nmid (d - 1)$ and $4 \mid (d - 1)$, as well as $d < 0$ and $d > 0$. In particular, the Gaussian and the Eisenstein integers are Euclidean.

Proof. Note first that the multiplicativity of the norm map $N\colon \mathcal{O}_d \to \mathbb{Z}$ implies monotonicity. Hence we only have to show that this allows for quotient and remainder. To do so, we distinguish the cases $4 \nmid (d-1)$ and $4 \mid (d-1)$.

i) If $d \in \{-2,-1,2,3\}$, then $\mathcal{O}_d = \mathbb{Z}[\sqrt{d}]$. Let $u, v \in \mathbb{Z}[\sqrt{d}]$ such that $v \neq 0$. Then let $uv^{-1} = s + t\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$ for some $s, t \in \mathbb{Q}$, and let $x, y \in \mathbb{Z}$ such that $|s-x| \leq \frac{1}{2}$ and $|t-y| \leq \frac{1}{2}$. Let $q := x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ and $r := u - qv \in \mathbb{Z}[\sqrt{d}]$. Then we have $r = v \cdot (uv^{-1} - q) = v \cdot \big((s-x) + (t-y)\sqrt{d}\big)$. Since $|(s-x)^2 - d(t-y)^2| \leq \frac{1}{4} + 2 \cdot \frac{1}{4} < 1$ for $|d| \leq 2$, and $-\frac{3}{4} \leq (s-x)^2 - 3(t-y)^2 \leq \frac{1}{4}$ for $d = 3$, we get $|N(r)| = |N(v)| \cdot |N(uv^{-1} - q)| = |N(v)| \cdot |(s-x)^2 - d(t-y)^2| < |N(v)|$.

ii) If $d \in \{-11,-7,-3,5,13\}$, then $\mathcal{O}_d = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. Let $u, v \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ such that $v \neq 0$. Let again $uv^{-1} = s + t\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$ for some $s, t \in \mathbb{Q}$, let $y \in \mathbb{Z}$ such that $|2t - y| \leq \frac{1}{2}$, then let $x \in \mathbb{Z}$ such that $|s - x - \frac{y}{2}| \leq \frac{1}{2}$. Let $q := x + y\frac{1+\sqrt{d}}{2} \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ and $r := u - qv \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. Since $|(s-x-\frac{y}{2})^2 - d(t-\frac{y}{2})^2| \leq \frac{1}{4} + 11 \cdot \frac{1}{16} < 1$ for $|d| \leq 11$, and $-\frac{13}{16} \leq (s - x - \frac{y}{2})^2 - 13(t - \frac{y}{2})^2 \leq \frac{1}{4}$ for $d = 13$, we get $|N(r)| = |N(v)| \cdot |N(uv^{-1} - q)| = |N(v)| \cdot |(s - x - \frac{y}{2})^2 - d(t - \frac{y}{2})^2| < |N(v)|$. ♯

Theorem. a) For $d \leq -13$ the ring $\mathcal{O}_d$ is not Euclidean. Hence for $d < 0$ the ring $\mathcal{O}_d$ is Euclidean if and only if it is Euclidean with respect to the norm map.

b) For $d > 0$ the ring $\mathcal{O}_d$ is Euclidean with respect to the norm map if and only if $d \in \{2,3,5,6,7,11,13,17,19,21,29,33,37,41,55,73\}$. ♯

In part a), it is not too difficult to see that for $d \leq -13$ the ring $\mathcal{O}_d$ is not Euclidean with respect to any degree map. (But still we do not prove this here.) Since for $d \in \{-5,-6,-10\}$ we have already seen in (5.4) that the ring $\mathcal{O}_d = \mathbb{Z}[\sqrt{d}]$ is not factorial, let alone Euclidean, the second assertion follows.

In part b), generalising the method used to prove the preceeding theorem, it is not too difficult to see that for $d \in \{2,3,5,6,7,13,17,21,29\}$ the ring $\mathcal{O}_d$ is Euclidean with respect to the norm map. (But still we do not prove this here.) The full assertion, buildung on quite a few predecessors, was finally proved by Inkeri [1949] and Chatland–Davenport [1950]. But it still is an open problem whether there is a real quadratic number ring which is Euclidean, but not Euclidean with respect to the norm map; actually, the factorial domain $\mathcal{O}_{14}$ is considered to be a possible candidate.

6 Applications

We present a few applications of quadratic number rings. The first one comes quite unexpected, in preparation of which we determine a group of units first:

(6.1) Example. Let $d := 2$ and $\epsilon := 1 + \sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Then we have $\mathbb{Z}[\sqrt{2}]^* = \{\pm\epsilon^k \in \mathbb{Z}[\sqrt{2}]; k \in \mathbb{Z}\}$, where the elements given are pairwise different.

Proof. We have $N(\epsilon) = -1$, thus $\pm\epsilon^k \in \mathbb{Z}[\sqrt{2}]^*$ for all $k \in \mathbb{Z}$. Conversely, if $z = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]^*$, by going over to $\pm z$ or $\pm z^{-1} = \pm N(z) \cdot \kappa(z)$ if necessary we may assume that $a, b \geq 0$. We are going to show that $z = \epsilon^k$ for some $k \in \mathbb{N}_0$. To this end, we use induction on $a + b \in \mathbb{N}$, where we have $a + b = 1$ if and only if $b = 0$, in which case $a = 1$ and thus $z = 1 = \epsilon^0$. Hence let now $a + b \geq 2$:

We next show that $b \leq a \leq 2b$: Assuming to the contrary that $0 \leq a < b$, we get $2b^2 \pm 1 = a^2 < b^2$, hence $b^2 < \mp 1$, thus $b = 0$, a contradiction; assuming to the contrary that $a > 2b > 0$, we get $2b^2 \pm 1 = a^2 > 4b^2$, hence $2b^2 < \pm 1$, thus $b = 0$, a contradiction. Now we have $\epsilon^{-1} = -\kappa(\epsilon) = -1 + \sqrt{2}$, thus $z\epsilon^{-1} = (a + b\sqrt{2})(-1 + \sqrt{2}) = (2b - a) + (a - b)\sqrt{2}$, where both $2b - a \geq 0$ and $a - b \geq 0$. Since $(2b - a) + (a - b) = b < a + b$, by induction there is $k \in \mathbb{N}_0$ such that $z\epsilon^{-1} = \epsilon^k$, hence $z = \epsilon^{k+1}$.

It remains to be shown that the elements $\pm\epsilon^k \in \mathbb{Z}[\sqrt{2}]^*$ are pairwise different, for all $k \in \mathbb{Z}$: Since $\epsilon^{-k} = (\epsilon^{-1})^k = (-\kappa(\epsilon))^k = (-1)^k\kappa(\epsilon^k)$, and $\epsilon^k \in \mathbb{Z}$ if and only if $k = 0$, it again suffices to consider the elements $\epsilon^k \in \mathbb{Z}[\sqrt{2}]^*$ for $k \in \mathbb{N}_0$. But now letting $\epsilon^k = a + b\sqrt{2}$ for $a, b \in \mathbb{Z}$, we get $\epsilon^{k+1} = (a + b\sqrt{2})(1 + \sqrt{2}) = (a + 2b) + (a + b)\sqrt{2}$, which by induction on $k \in \mathbb{N}_0$ implies that $a, b \geq 0$, and that $a + b$ is strictly increasing with k. ♯

The above considerations yield recursion formulae to compute the coefficients $a_k, b_k \in \mathbb{N}_0$ of $\epsilon^k = a_k + b_k\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, namely $a_{k+1} := a_k + 2b_k$ and $b_{k+1} := a_k + b_k$ for $k \in \mathbb{N}_0$, where $a_0 = 1$ and $b_0 = 0$. Hence both sequences $[a_0, a_1, \ldots]$ and $[b_0, b_1, \ldots]$ are strictly increasing, where a_k is odd, while b_{2k} is even and b_{2k+1} is odd, for $k \in \mathbb{N}_0$. A few explicit values are given in Table 5.

We are now prepared for our application, keeping the notation used:

(6.2) Example. Amongst the sums $s_n := \sum_{i=1}^{n} i = 1 + 2 + \cdots + n \in \mathbb{N}$, where $n \in \mathbb{N}$, there are infinitely many squares.

Proof. We are actually able to describe the squares occurring precisely, which in particular shows that there are infinitely of them; a few values are given in Table 5. To this end, let $n \in \mathbb{N}$ such that $\frac{n(n+1)}{2} = s_n = s^2$, for some $s \in \mathbb{N}$, or equivalently $n(n + 1) = 2s^2$; note that $\gcd_+(n, n + 1) = 1$.

i) Let n be odd. Then we have $n = m^2$ for some odd $m \in \mathbb{N}$ such that $m \mid s$, and we let $l \in \mathbb{N}$ such that $ml = s$. From $n(n+1) = 2s^2$ we get $n - \frac{2s^2}{n} = -1$, which yields $m^2 - 2l^2 = -1$. Hence there is $k \in \mathbb{N}$ odd such that $\epsilon^k = m + l\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Conversely, given $\epsilon^k = m + l\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ for some $k \in \mathbb{N}$ odd, we obtain $n := m^2$ and $s := ml$ fulfilling $-1 = m^2 - 2l^2 = n - \frac{2s^2}{n}$, hence $n(n + 1) = 2s^2$.

ii) Let n be even. Then let $n' := n + 1$. Hence n' being odd we have $n' = m^2$ for some odd $m \in \mathbb{N}$ such that $m \mid s$, and we let $l \in \mathbb{N}$ such that $ml = s$. From $(n' - 1)n' = 2s^2$ we get $n' - \frac{2s^2}{n'} = 1$, which yields $m^2 - 2l^2 = 1$. Hence there is $k \in \mathbb{N}$ even such that $\epsilon^k = m + l\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Conversely, given

Table 5: Units $\epsilon^k = a_k + b_k\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$.

k	a_k	b_k	n	$s = \sqrt{s_n}$
0	1	0	0	0
1	1	1	1	1
2	3	2	8	6
3	7	5	49	35
4	17	12	288	204
5	41	29	1681	1189
6	99	70	9800	6930
7	239	169	57121	40391
8	577	408	332928	235416
9	1393	985	1940449	1372105
10	3363	2378	11309768	7997214
11	8119	5741	65918161	46611179
12	19601	13860	384199200	271669860
13	47321	33461	2239277041	1583407981
14	114243	80782	13051463048	9228778026
15	275807	195025	76069501249	53789260175

$\epsilon^k = m + l\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ for some $k \in \mathbb{N}$ even, we obtain $n := m^2 - 1$ and $s := ml$ fulfilling $1 = m^2 - 2l^2 = (n+1) - \frac{2s^2}{n+1}$, hence $n(n+1) = 2s^2$. ♯

Next we consider a couple of diophantine equations, whose solutions are found using the Euclidean domains $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{-2}]$, respectively:

(6.3) Example: Diophantine equations. a) The equation $X^3 = Y^2 + 1$ has only the integer solutions $x = 1$ and $y = 0$. In other words, $n = 0$ is the only square integer such that $n + 1$ is a cube.

b) The equation $X^3 = Y^2 + 2$ has only the integer solutions $x = 3$ and $y \in \{\pm 5\}$. (This fact was reportedly already known to FERMAT.) In other words, $n = 26$ is the only integer such that $n - 1$ is a square and $n + 1$ is a cube.

Proof. a) Let $[x, y] \in \mathbb{Z}^2$ be a solution. We go over to the ring $\mathbb{Z}[i]$, which is Euclidean, hence factorial. We have $x^3 = y^2 + 1 = (y - i)(y + i) \in \mathbb{Z}[i]$.

Let $\gamma \in \gcd(y - i, y + i)$, then $\gamma \mid \big((y + i) - (y - i)\big) = 2i = (1 + i)^2 \in \mathbb{Z}[i]$. Hence we have $\gamma \sim 1$ or $\gamma \sim (1 + i)$ or $\gamma \sim (1 + i)^2$; note that $N(1 + i) = 2 \in \mathbb{Z}$ indecomposable implies that $(1 + i) \in \mathbb{Z}[i]$ is indecomposable. Moreover, since $1 - i = -i(1 + i) \sim 1 + i$, using the conjugation map we infer $\nu_{1+i}(y + i) = \nu_{1-i}(y - i) = \nu_{1+i}(y - i)$, hence $3 \mid \nu_{1+i}(x^3) = 2\nu_{1+i}(y + i)$, thus $3 \mid \nu_{1+i}(y + i)$.

Let $\pi \in \mathbb{Z}[i]$ be indecomposable such that $\pi \not\sim (1 + i)$. Then $\pi \nmid \gamma \in \mathbb{Z}[i]$, hence

π divides at most one of $1\pm i$, thus $3 \mid \nu_\pi(x^3) = \nu_\pi(y+i)$. Since $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$ consists of cubes, we infer that $y + i \in \mathbb{Z}[i]$ is a cube. There are $a, b \in \mathbb{Z}$ such that $y+i = (a+bi)^3 = a(a^2-3b^2)+b(3a^2-b^2)i \in \mathbb{Z}[i]$, implying $b(3a^2-b^2) = 1$, hence $b = -1$ and $a = 0$, and thus $y = a(a^2 - 3b^2) = 0$.

b) Let $[x, y] \in \mathbb{Z}^2$ be a solution. Assume that y is even, then $y^2 + 2$ is even, but not divisible by 4; hence x is even, thus x^3 is divisible by 8, a contradiction. Hence y is odd. Now we go over to the ring $\mathbb{Z}[\sqrt{-2}]$, which is Euclidean, hence factorial. We have $x^3 = y^2 + 2 = (y - \sqrt{-2})(y + \sqrt{-2}) \in \mathbb{Z}[\sqrt{-2}]$. We next show that $y - \sqrt{-2}$ and $y + \sqrt{-2}$ are coprime in $\mathbb{Z}[\sqrt{-2}]$:

Let $c + d\sqrt{-2} \in \gcd(y - \sqrt{-2}, y + \sqrt{-2})$, then $(c + d\sqrt{-2}) \mid \big((y + \sqrt{-2}) + (y - \sqrt{-2})\big) = 2y \in \mathbb{Z}[\sqrt{-2}]$ and $(c + d\sqrt{-2}) \mid \big((y + \sqrt{-2}) - (y - \sqrt{-2})\big) = 2\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$. Taking norms yields $c^2 + 2d^2 \mid 4y^2 \in \mathbb{Z}$ and $c^2 + 2d^2 \mid 8 \in \mathbb{Z}$, implying $c^2+2d^2 \mid \gcd_+(4y^2, 8) = 4 \in \mathbb{Z}$. Hence $[c, d] \in \{[0, \pm 1], [\pm 1, 0], [\pm 2, 0]\}$. Assume that $\sqrt{-2} \mid (y - \sqrt{-2}) \in \mathbb{Z}[\sqrt{-2}]$, then $\sqrt{-2} \mid y \in \mathbb{Z}[\sqrt{-2}]$, hence $2 \mid y^2 \in \mathbb{Z}$, a contradiction; assume that $2 \mid (y - \sqrt{-2}) \in \mathbb{Z}[\sqrt{-2}]$, then $\sqrt{-2} \mid (y - \sqrt{-2}) \in \mathbb{Z}[\sqrt{-2}]$, which is known to be a contradiction. Hence we have $c+d\sqrt{-2} \in \{\pm 1\}$.

Since $\mathbb{Z}[\sqrt{-2}]^* = \{\pm 1\}$ consists of cubes, we infer that both $y \pm \sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$ are cubes, thus there is $a + b\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$ such that $(a + b\sqrt{-2})^3 = y + \sqrt{-2}$, where the left hand side equals $(a + b\sqrt{-2})^3 = a(a^2 - 6b^2) + b(3a^2 - 2b^2)\sqrt{-2}$. This yields $a(a^2-6b^2) = y$ and $b(3a^2-2b^2) = 1$. Hence we infer $|b| = 1$. Assume that $b = -1$, then $3a^2 = 1$, a contradiction. Thus we have $b = 1$, hence $3a^2 = 3$, entailing $a \in \{\pm 1\}$. Hence we have $y = a(a^2 - 6b^2) \in \{\mp 5\}$, and $x = 3$. ♯

(6.4) Example: Gaussian primes. We proceed to determine the primes in $\mathbb{Z}[i]$. Recall that $\mathbb{Z}[i]$ is Euclidean, hence is a principal ideal domain, and thus is factorial. Conjugation is given as $\kappa\colon \mathbb{Z}[i] \to \mathbb{Z}[i]\colon a + bi \mapsto a - bi$, and the norm map is $N\colon \mathbb{Z}[i] \to \mathbb{Z}\colon a + bi \mapsto (a + bi)(a - bi) = a^2 + b^2$. Moreover, we have $\mathbb{Z}[i]^* = \{z \in \mathbb{Z}[i]; N(z) = 1\} = \{\pm 1, \pm i\}$.

Lemma. Let $\pi \in \mathbb{Z}[i]$ be a prime. Then there is a unique $p \in \mathcal{P} \subseteq \mathbb{Z}$ such that $\pi \mid p \in \mathbb{Z}[i]$, and we have $N(\pi) \in \{p, p^2\}$.

Proof. We have $N(\pi) \in \mathbb{Z}$ such that $N(\pi) > 1$. Hence considering the factorisation of $N(\pi) \in \mathbb{Z}$, from $N(\pi) = \pi \cdot \kappa(\pi)$ and $\pi \in \mathbb{Z}[i]$ being a prime we infer that $\pi \mid p \in \mathbb{Z}[i]$ for some prime $p \in \mathcal{P}$ such that $p \mid N(\pi) \in \mathbb{Z}$. Moreover, from $\pi \mid p$ we get $N(\pi) \mid N(p) = p^2$, hence $N(\pi) \in \{p, p^2\}$, which also shows that the prime $p \in \mathcal{P}$ such that $\pi \mid p \in \mathbb{Z}[i]$ is uniquely determined. ♯

The primes $\pi \in \mathbb{Z}[i]$ can be grouped according to the prime $p \in \mathcal{P}$ they divide:

Theorem. Let $\pi \in \mathbb{Z}[i]$ be a prime, and let $p \in \mathcal{P}$ such that $\pi \mid p \in \mathbb{Z}[i]$.

a) If $p = 2$, then we have $2 \sim (1 + i)^2$, in other words $\pi \in \{\pm 1 \pm i\}$ are the prime divisors of 2 in $\mathbb{Z}[i]$; the prime 2 is called **ramified** in $\mathbb{Z}[i]$.

b) If $4 \mid p+1$, then we have $\pi \sim p$, in other words $\pi \in \{\pm p, \pm ip\}$ are the prime divisors of p in $\mathbb{Z}[i]$; the prime p is called **inert** in $\mathbb{Z}[i]$.

c) If $4 \mid p-1$, then we have $p = \pi \cdot \kappa(\pi)$, where $\pi \not\sim \kappa(\pi)$, in other words $\{\pm\pi, \pm i\pi, \pm\kappa(\pi), \pm i\kappa(\pi)\}$ are the prime divisors of p in $\mathbb{Z}[i]$; the prime p is called **split** in $\mathbb{Z}[i]$.

Proof. a) Let $p = 2$. From $N(1+i) = 2$ we infer that $1+i \in \mathbb{Z}[i]$ is a prime, and hence we have the factorisation $(1+i)^2 \sim (1+i)(1-i) = 2 \in \mathbb{Z}[i]$. This implies $\pi \sim 1+i$.

b) Let $4 \mid p+1$. Assume that $N(\pi) = p$, then writing $\pi = a + ib$, for some $a, b \in \mathbb{Z}$, yields $a^2 + b^2 = p$. We have $a = a' + 4k$ and $b = b' + 4l$, for some $a', b' \in \{0, \ldots, 3\}$ and $k, l \in \mathbb{Z}$. From this we get $a^2 + b^2 = c + 4m$, for some $c \in \{0, 1, 2\}$ and $m \in \mathbb{Z}$, thus $4 \nmid a^2 + b^2 + 1$, a contradiction. Hence we have $N(\pi) = p^2 = N(p)$, entailing $\pi \sim p$.

c) Let $4 \mid p-1$. Then by (10.6), as a consequence of Artin's Theorem, the quadratic congruence $X^2 + 1 \equiv 0 \pmod{p}$ is solvable, hence let $x \in \mathbb{Z}_p$ such that $p \mid x^2 + 1$. We consider the ideal $I := \langle p, x+i \rangle \trianglelefteq \mathbb{Z}[i]$. Since $\mathbb{Z}[i]$ is a principal ideal domain, we have $I = \langle \pi \rangle$ where $\pi \in \gcd(p, x+i) \subseteq \mathbb{Z}[i]$.

For any $z \in I$ there are $\alpha, \beta \in \mathbb{Z}[i]$ such that $z = p\alpha + (x+i)\beta$, hence we have $N(z) = N\big(p\alpha + (x+i)\beta\big) = \big(p\alpha + (x+i)\beta\big) \cdot \big(p\kappa(\alpha) + (x-i)\kappa(\beta)\big) = pN(\alpha) + (x^2+1)N(\beta) + p(x-i)\alpha\kappa(\beta) + p(x+i)\kappa(\alpha)\beta$, showing that $p \mid N(z) \in \mathbb{Z}[i]$. In particular, $\pi \in \mathbb{Z}[i]$ is not a unit, that is $N(\pi) > 1$.

Since $\pi \mid p$ and $\pi \mid x+i$ we have $N(\pi) \mid N(p) = p^2$ and $N(\pi) \mid N(x+i) = (x+i)(x-i) = x^2 + 1$. Since $x^2 + 1 \leq (p-1)^2 + 1 = p^2 - 2(p-1) < p^2$, we have $N(\pi) < p^2$, hence we conclude that $N(\pi) = p$.

Thus in particular $\pi \in \mathbb{Z}[i]$ is a prime. Assume that $\pi \sim \kappa(\pi)$, then $\pi \sim \kappa(\pi) \mid \kappa(x+i) = x - i$, hence $\pi \mid \big((x+i) - (x-i)\big) = 2i$, implying $N(\pi) \mid N(2i) = 4$, a contradiction. Thus we have $\pi \not\sim \kappa(\pi)$. Hence from $\kappa(\pi) \mid \kappa(p) = p$ we get $\pi \cdot \kappa(\pi) \mid p$. Since $N(\pi \cdot \kappa(\pi)) = p^2 = N(p)$, we conclude that $\pi \cdot \kappa(\pi) \sim p$. ♯

In the last case, if $4 \mid p-1$, writing $\pi = a + bi \in \mathbb{Z}[i]$ for some $a, b \in \mathbb{Z}$, from $N(\pi) = a^2 + b^2 = p$ we get $a, b \neq 0$ and $a \neq b$, and the prime divisors of p are given as $\{\pm\pi, \pm i\pi, \pm\kappa(\pi), \pm i\kappa(\pi)\} = \{\pm a \pm ib, \pm b \pm ia\}$.

Moreover, π is found as follows: We first determine $x \in \mathbb{Z}_p$ such that $p \mid x^2 + 1$, subsequently we compute $\pi \in \gcd(p, x+i) \subseteq \mathbb{Z}[i]$ using the Euclidean algorithm; actually, by Wilson's Theorem, see (10.5), we have $x = \big((\pm(\frac{p-1}{2})!) \bmod p\big)$.

Corollary. A prime $p \in \mathcal{P}$ is a sum of two squares in $\mathbb{Z}$ if and only if $p = 2$ or $4 \mid p-1$. In this case, there is a unique representation $p = a^2 + b^2$, where $a, b \in \mathbb{N}$ such that $a \leq b$. ♯

This yields the following application to a question of integer arithmetic:

(6.5) Theorem: Euler's two-squares theorem [1754].
Let $n = 2^c \cdot \prod_{i=1}^{r} p_i^{a_i} \cdot \prod_{j=1}^{s} q_j^{b_j} \in \mathbb{N}$, where $p_i, q_j \in \mathcal{P}$ are pairwise distinct odd primes, such that $4 \mid p_i - 1$ and $4 \mid q_j + 1$, and where $c \in \mathbb{N}_0$ and $a_i, b_j \in \mathbb{N}$, for some $r, s \in \mathbb{N}_0$.

a) Then n is a sum of two squares in $\mathbb{Z}$ if and only if $b_1, \ldots, b_s$ are all even.

b) There is a **primitive** representation $n = a^2 + b^2$, that is $a, b \in \mathbb{Z}$ such that $\gcd_+(a, b) = 1$, if and only if $c \in \{0, 1\}$ and $s = 0$. In this case, if $r \geq 1$ there are precisely 2^{r-1} primitive representations such that $a, b \in \mathbb{N}$ such that $a \leq b$; if $r = 0$ then $1 = 0^2 + 1^2$ and $2 = 1^2 + 1^2$ have a unique such representation.

Proof. a) If $n = a^2 + b^2 = N(a + bi) = (a + bi) \cdot \kappa(a + bi)$, where $a, b \in \mathbb{Z}$, then we have the factorisation $a + bi \sim (1+i)^c \cdot \prod_{i=1}^{r} \left(\pi_i^{\alpha_i} \cdot \kappa(\pi_i)^{\alpha_i'}\right) \cdot \prod_{j=1}^{s} q_j^{\frac{b_j}{2}} \in \mathbb{Z}[i]$, where $p_i \sim \pi_i \cdot \kappa(\pi_i) \in \mathbb{Z}[i]$, and $\alpha_i, \alpha_i' \in \mathbb{N}_0$ such that $\alpha_i + \alpha_i' = a_i$, for all $i \in \{1, \ldots, r\}$. Hence b_j is even, for all $j \in \{1, \ldots, s\}$. Conversely, if the latter condition holds, then any element of $\mathbb{Z}[i]$ having a factorisation as above gives rise to a decomposition of n as a sum of two squares in $\mathbb{Z}$.

b) If n has a primitive representation, then from $2^{(c \text{ div } 2)} \cdot \prod_{j=1}^{s} q_j^{\frac{b_j}{2}} \mid \gcd_+(a, b)$ we get $c \leq 1$ and $s = 0$. Hence let $a + bi \sim (1 + i)^c \cdot \prod_{i=1}^{r} \left(\pi_i^{\alpha_i} \cdot \kappa(\pi_i)^{\alpha_i'}\right)$, where $c \leq 1$; we may assume that $r \geq 1$. Then we have $\gcd_+(a, b) > 1$ if and only if there is $p \in \mathcal{P}$ such that $p \mid a + bi \in \mathbb{Z}[i]$. From the given factorisation of $a + bi$ we infer that this is equivalent to having $\pi_i \cdot \kappa(\pi_i) \sim p_i \mid a + bi$ for some $i \in \{1, \ldots, r\}$, which in turn amounts to say that both $\alpha_i, \alpha_i' > 0$. Hence the primitive representations are precisely given by chosing $\{\alpha_i, \alpha_i'\} = \{a_i, 0\}$ for all $i \in \{1, \ldots, r\}$. Thus there are 2^r choices, which by interchanging all of the α_i and α_i' consist of 2^{r-1} pairs of mutually conjugate ones. ♯

Example. For $p := 5$ we get $x := 2$, hence $N(x + i) = 5 = p$ shows that $\pi \sim 2+i \in \mathbb{Z}[i]$; thus we get $5 = 1^2+2^2$. For $p := 13$ we get $x := 5$, then quotient and remainder yields $p = (3-i)(x+i)-(3-2i)$, hence $N(3+2i) = 13 = p$ shows that $\pi \sim 3+2i \in \mathbb{Z}[i]$; thus we get $13 = 2^2+3^2$. Thus for $n := 65 = 5 \cdot 13$, up to conjugation we get $a+bi \sim (2+i)(3+2i) = 4+7i$ and $a+bi \sim (2+i)(3-2i) = 8-i$, which hence yield $65 = 4^2 + 7^2 = 1^2 + 8^2$.

(6.6) Sums of squares. By Euler's Theorem there are infinitely many positive integers which are a sum of two squares in $\mathbb{Z}$. But since there are infinitely many primes kongruent to 3 modulo 4, see (13.1), there also infinitely many positive integers which cannot be written as a sum of two squares in $\mathbb{Z}$.

Hence, firstly we may ask, how 'dense' the set of positive integers which are a sum of two squares in $\mathbb{Z}$ is as a subset of all positive integers: Letting $\sigma_2(x) := |\{n \in \mathbb{N}; n \leq x, n = a^2 + b^2 \text{ for some } a, b \in \mathbb{Z}\}|$, for $x \in \mathbb{R}_{>0}$, due to Landau [1909] we have $\lim_{x\to\infty} \left(\sigma_2(x) \cdot \frac{\sqrt{\ln(x)}}{x}\right) = c > 0$, hence $\lim_{x\to\infty} \frac{\sigma_2(x)}{x} = 0$. (This we do not prove here.)

Secondly, we wonder whether allowing for more summands changes the picture, and we may ask whether there is a fixed number $s \in \mathbb{N}$ such that any positive integer can be written as a sum of s squares in $\mathbb{Z}$. Since $7 = 1^2 + 1^2 + 1^2 + 2^2$ is the only way of writing 7 non-trivially as a sum of squares in $\mathbb{Z}$, we conclude that $s \geq 4$, if it exists at all. Indeed s exists, and we have $s = 4$ by the following theorem (which is not proven here either):

Theorem: Lagrange's four-squares theorem [1770].
Any positive integer can be written as a sum of four squares in $\mathbb{Z}$. ♯

III Congruences

7 Residue classes

(7.1) Residue class rings. a) Let $n \in \mathbb{N}$. We consider the relation $\mathcal{M}_n := \{[a,b] \in \mathbb{Z}^2; (a \bmod n) = (b \bmod n) \in \mathbb{Z}_n\}$, where $\mathbb{Z}_n := \{0, \dots, n-1\}$; in this case we write $a \equiv b \pmod{n}$. In other words, for $a, b \in \mathbb{Z}$ we have $a \equiv b \pmod{n}$, if and only if a and b have the same remainder upon division by n.

Then $\mathcal{M}_n$ is an equivalence relation on $\mathbb{Z}$, that is $\mathcal{M}_n$ is reflexive, symmetric and transitive. The associated equivalence classes $\overline{a} = [a]_n = \{b \in \mathbb{Z}; (a \bmod n) = (b \bmod n)\} \subseteq \mathbb{Z}$, for $a \in \mathbb{Z}$, are called **residue classes modulo** n.

Lemma. For $a \in \mathbb{Z}$ we have $\overline{a} = \{a + kn \in \mathbb{Z}; k \in \mathbb{Z}\} = \{b \in \mathbb{Z}; n \mid (a-b)\}$.

Proof. Let $b \in \overline{a}$, then there are $c \in \mathbb{Z}_n$ and $r, s \in \mathbb{Z}$ such that $a = c + rn$ and $b = c + sn$, hence $b = a + (s-r)n$; this shows $\overline{a} \subseteq \{a + kn \in \mathbb{Z}; k \in \mathbb{Z}\}$. Let $k \in \mathbb{Z}$, then $n \mid kn = \big((a+kn) - a\big)$ shows $\{a + kn \in \mathbb{Z}; k \in \mathbb{Z}\} \subseteq \{b \in \mathbb{Z}; n \mid (a-b)\}$.

Let finally $b \in \mathbb{Z}$ such that $n \mid (a-b)$, and let $c, d \in \mathbb{Z}_n$ and $r, s \in \mathbb{Z}$ such that $a = c + rn$ and $b = d + sn$, then $n \mid \big((a-b) + (r-s)n\big) = c - d$. Hence from $|c - d| < n$ we conclude $c = d$, showing that $\{b \in \mathbb{Z}; n \mid (a-b)\} \subseteq \overline{a}$. ♯

b) Hence we also write $\overline{a} = a + n\mathbb{Z} := \{a + kn \in \mathbb{Z}; k \in \mathbb{Z}\} \subseteq \mathbb{Z}$. Now let $\mathbb{Z}/n\mathbb{Z} := \{a + n\mathbb{Z} \subseteq \mathbb{Z}; a \in \mathbb{Z}\}$ be the set of residue classes. This gives rise to the **natural map** $\nu_n \colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \colon a \mapsto a + n\mathbb{Z}$; note that ν_n is surjective.

Then quotient and remainder shows that $\mathbb{Z}/n\mathbb{Z} = \{a + n\mathbb{Z} \subseteq \mathbb{Z}; a \in \mathbb{Z}_n\} = \{\overline{0}, \dots, \overline{n-1}\}$. Moreover, since $(a \bmod n) = a$ for $a \in \mathbb{Z}_n$, we conclude that the latter residue classes are pairwise different. Thus $\mathbb{Z}_n$ is a set of **representatives** of the residue classes modulo n, that is the natural map induces a bijection $\mathbb{Z}_n \to \mathbb{Z}/n\mathbb{Z}$, and hence we have the disjoint union $\mathbb{Z} = \coprod_{a \in \mathbb{Z}_n} (a + n\mathbb{Z})$.

For example, for $n = 2$ the equivalence classes are $0 + 2\mathbb{Z} = \{0, 2, -2, 4, -4, \dots\}$ and $1 + 2\mathbb{Z} = \{1, -1, 3, -3, \dots\}$, that is the even and odd integers, respectively.

Proposition. Let $n \in \mathbb{N}$.

a) The set $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \dots, \overline{n-1}\}$ is a commutative ring, being called the associated **residue class ring**, with addition $\overline{a} + \overline{b} := \overline{a+b}$ and multiplication $\overline{a} \cdot \overline{b} := \overline{ab}$, for $a, b \in \mathbb{Z}$, with additive neutral element $\overline{0}$, the additive inverse of $\overline{a}$ being $\overline{-a}$, and multiplicative neutral element $\overline{1}$.

Moreover, the natural map $\nu_n \colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \colon a \mapsto \overline{a}$ is a surjective ring homomorphism such that $\ker(\nu_n) = n\mathbb{Z} \trianglelefteq \mathbb{Z}$.

b) The set $\mathbb{Z}_n = \{0, \dots, n-1\}$ is a commutative ring, with addition $a + b := \big((a+b) \bmod n\big)$ and multiplication $a \cdot b := \big((ab) \bmod n\big)$, for $a, b \in \mathbb{Z}_n$, with additive neutral element 0, the additive inverse of a being $\big((-a) \bmod n\big)$ and multiplicative neutral element 1.

Moreover, the map $\nu_n|_{\mathbb{Z}_n} \colon \mathbb{Z}_n \to \mathbb{Z}/n\mathbb{Z} \colon a \mapsto \overline{a}$ is a ring isomorphism.

Proof. a) Noting that $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ is an ideal, the assertion follows from the homomorphism theorem, but we prefer to give an explicit proof. To this end, we only have to show that addition and multiplication are independent of the choice of representatives of the equivalence classes; then the rules of arithmetic in $\mathbb{Z}/n\mathbb{Z}$ are inherited from those in $\mathbb{Z}$ via the natural map:

Let $a, a', b, b' \in \mathbb{Z}$ such that $\overline{a} = \overline{a'}$ and $\overline{b} = \overline{b'}$, that is there are $k, l \in \mathbb{Z}$ such that $a' = a + kn$ and $b' = b + ln$. Hence we have $a' + b' = (a + kn) + (b + ln) = (a + b) + (k + l)n$ and $a'b' = (a + kn)(b + ln) = ab + (al + bk + kln)n$, thus $\overline{a' + b'} = \overline{a + b}$ and $\overline{a'b'} = \overline{ab}$.

In particular, the natural map becomes a ring homomorphism. Moreover, for $k \in \mathbb{Z}$ we have $\nu_n(kn) = \overline{kn} = \overline{0}$, hence $n\mathbb{Z} \subseteq \ker(\nu_n)$; conversely, for $a \in \ker(\nu_n)$ we have $\overline{a} = \nu_n() = \overline{0}$, hence $a = kn$ for some $k \in \mathbb{Z}$, showing that $\ker(\nu_n) \subseteq n\mathbb{Z}$.

b) We have already seen that restricting the natural map yields the bijection $\omega_n := \nu_n|_{\mathbb{Z}_n} \colon \mathbb{Z}_n \to \mathbb{Z}/n\mathbb{Z} \colon a \mapsto \overline{a}$. Hence $\mathbb{Z}_n$ becomes a commutative ring by **transport of structure**, that is by letting $a + b := \omega_n^{-1}(\omega_n(a) + \omega_n(b)) = \omega_n^{-1}(\overline{a} + \overline{b}) = \omega_n^{-1}(\overline{a+b}) = ((a+b) \bmod n)$ and $a \cdot b := \omega_n^{-1}(\omega_n(a) \cdot \omega_n(b)) = \omega_n^{-1}(\overline{a} \cdot \overline{b}) = \omega_n^{-1}(\overline{a \cdot b}) = ((a \cdot b) \bmod n)$, for $a, b \in \mathbb{Z}_n$, the additive and multiplicative neutral elements being given by $\omega_n^{-1}(\overline{0}) = 0$ and $\omega_n^{-1}(\overline{1}) = 1$, respectively. This also shows that ω_n is a ring homomorphism. ♯

Note that $\mathbb{Z}/n\mathbb{Z}$ is the zero ring if and only if $n = 1$. Addition and multiplication in the rings $\mathbb{Z}/n\mathbb{Z}$, where $n \in \{2, \dots, 5\}$, are as given below; note that the case $n = 2$ is reminiscent of boolean algebra, by identfiying 0 and 1 with the logical values false and true, respectively, and '+' and '·' with the logical operations

exclusive or and and, respectively:

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

(7.2) Example: Fermat numbers. For $n \in \mathbb{N}_0$ let $F_n := 2^{2^n} + 1 \in \mathbb{N}$ be the n-th **Fermat number**. Then $F_0 = 2^1+1 = 3$, $F_1 = 2^2+1 = 5$, $F_2 = 2^4+1 = 17$, $F_3 = 2^8 + 1 = 257$, $F_4 = 2^{16} + 1 = 65537$ are all primes, and it was conjectured by Fermat [1640] that F_n always is a prime.

Nowadays, all F_n for $n \in \{5, \dots, 32\}$ are known to be composite, but it still is an open problem whether $\{F_0, \dots, F_4\}$ are the only Fermat primes. Even worse, complete factorisations are only known for $n \leq 11$; see also (13.3).

For example, the Fermat number $F_5 = 2^{32}+1 = 4\,294\,967\,297 \sim 4 \cdot 10^9$ factorises as $F_5 = 641 \cdot 6\,700\,417$ [Euler, 1732]. Having the candidate divisor 641 in our hands, we may prove that actually $641 \mid F_5$ by showing that $\overline{F_5} = \overline{0} \in \mathbb{Z}/641\mathbb{Z}$:

We have $641 = 640 + 1 = 5 \cdot 2^7 + 1$, thus $\overline{5 \cdot 2^7} = -\overline{1} \in \mathbb{Z}/641\mathbb{Z}$, and $641 = 625+16 = 5^4+2^4$, thus $\overline{2}^4 = -\overline{5}^4 \in \mathbb{Z}/641\mathbb{Z}$, hence $\overline{F_5} = \overline{2}^{32} + \overline{1} = \overline{2}^4 \cdot \overline{2}^{28} + \overline{1} = -\overline{5}^4 \cdot \overline{2^7}^4 + \overline{1} = -\overline{5 \cdot 2^7}^4 + \overline{1} = -(-\overline{1})^4 + \overline{1} = -\overline{1} + \overline{1} = \overline{0} \in \mathbb{Z}/641\mathbb{Z}$. ♯

(7.3) Theorem. Let $n \in \mathbb{N}$.

a) Then $\overline{0} \neq \overline{a} \in \mathbb{Z}/n\mathbb{Z}$ is a zero-divisor if and only if $\gcd_+(a, n) > 1$.

b) The group of units of $\mathbb{Z}/n\mathbb{Z}$ equals $(\mathbb{Z}/n\mathbb{Z})^* = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z}; \gcd_+(a, n) = 1\}$. Hence the latter is also called the group of **prime residues classes** modulo n.

In particular, this shows that $\mathbb{Z}/n\mathbb{Z}$ is an integral domain if and only if $\mathbb{Z}/n\mathbb{Z}$ is a field, which holds if and only if n is a prime.

Proof. Note that the greatest common divisors occurring in the assertions are indeed independent of the residue class representatives chosen: If $a, a' \in \mathbb{Z}$ such that $\overline{a} = \overline{a'} \in \mathbb{Z}/n\mathbb{Z}$, then we have $a' = a + kn$ for some $k \in \mathbb{N}$, and thus $\gcd(a', n) = \gcd(a + kn, n) = \gcd(a, n) \subseteq \mathbb{Z}$. Moreover, note that for $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ we have $\gcd_+(a, n) \in \{1, \dots, n\}$, and $\gcd_+(a, n) = n$ if and only if $\overline{a} = \overline{0}$.

Since $\mathbb{Z}/n\mathbb{Z}$ is finite, we already know that any of its non-zero elements is either a zero-divisor or a unit. Hence the arguments to follow are somewhat redundant, but still we prefer to give them explicitly:

We show that $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ is a unit if and only if $\gcd_+(a,n) = 1$: Let $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$, then there is $\overline{b} \in \mathbb{Z}/n\mathbb{Z}$ such that $\overline{ab} = \overline{1} \in \mathbb{Z}/n\mathbb{Z}$, that is there is $k \in \mathbb{Z}$ such that $ab + kn = 1 \in \mathbb{Z}$, which implies that $\gcd_+(a,n) = 1$. Conversely, if $\gcd_+(a,n) = 1$ then there are Bézout coefficients $c, c' \in \mathbb{Z}$ such that $ac + nc' = 1 \in \mathbb{Z}$, hence we have $\overline{ac} = \overline{1} \in \mathbb{Z}/n\mathbb{Z}$, implying that $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$ such that $\overline{a}^{-1} = \overline{c} \in \mathbb{Z}/n\mathbb{Z}$.

We show that $\overline{0} \neq \overline{a} \in \mathbb{Z}/n\mathbb{Z}$ is a zero-divisor if and only if $\gcd_+(a,n) > 1$: Let $d := \gcd_+(a,n) > 1$, then there is $0 \neq b \in \mathbb{Z}_n$ such that $bd = n$, thus we have $n \mid ab$, hence $\overline{ab} = \overline{0} \in \mathbb{Z}/n\mathbb{Z}$, implying that $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ is a zero-divisor. Conversely, let $\gcd_+(a,n) = 1$, and let $\overline{b} \in \mathbb{Z}/n\mathbb{Z}$ such that $\overline{ab} = \overline{0} \in \mathbb{Z}/n\mathbb{Z}$, then we have $n \mid ab$, and since a and n are coprime we infer that $n \mid b$, that is $\overline{b} = \overline{0} \in \mathbb{Z}/n\mathbb{Z}$, which implies that $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ is not a zero-divisor.

The last assertion follows from observing that we have $\gcd_+(a,n) = 1$ for all $0 \neq a \in \mathbb{Z}_n$ if and only if n is indecomposable, that is a prime. ♯

Note that the above argument shows that the inverse of $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$ is found using the extended Euclidean algorithm: Computing $\gcd_+(a,n) = 1$ yields Bézout coefficients $c, c' \in \mathbb{Z}$ such that $ac + nc' = 1 \in \mathbb{Z}$, thus $\overline{a}^{-1} = \overline{c} \in \mathbb{Z}/n\mathbb{Z}$.

8 Linear congruences

(8.1) Theorem. Let $n \in \mathbb{N}$. Given $a, b \in \mathbb{Z}$, the **linear congruence** $aX \equiv b \pmod{n}$ has a solution, that is there is $x \in \mathbb{Z}$ such that $ax \equiv b \pmod{n}$, or equivalently $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ such that $\overline{ax} = \overline{b} \in \mathbb{Z}/n\mathbb{Z}$, if and only if $\gcd_+(a,n) \mid b$. In this case, but apart from this independently of the choice of b, there are precisely $\gcd_+(a,n)$ solutions $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$, or equivalently solutions $x \in \mathbb{Z}_n$.

Proof. Let $d := \gcd_+(a,n)$. We first show that the condition given is necessary: Given $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$, we have $\overline{ax} = \overline{b}$ if and only if there is $k \in \mathbb{Z}$ such that $ax = b + kn$; in particular in this case we have $d = \gcd_+(a,n) \mid ax - kn = b$.

To show sufficiency, we may now let $n', a', b' \in \mathbb{Z}$ such that $n = dn'$, $a = da'$ and $b = db'$. Then for a solution $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ of the linear congruence $aX \equiv b \pmod{n}$ we have $da'x = db' + kdn'$, for some $k \in \mathbb{Z}$, hence $a'x = b' + kn'$, that is $\overline{\overline{x}} \in \mathbb{Z}/n'\mathbb{Z}$ is a solution of the linear congruence $a'X \equiv b' \pmod{n'}$. Conversely, if $\overline{\overline{x}} \in \mathbb{Z}/n'\mathbb{Z}$ is a solution of the latter, from $a'x = b' + kn'$, for some $k \in \mathbb{Z}$, we infer $ax = b + kn$, thus $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ is a solution of the given linear congruence.

For the natural maps $\nu_n \colon \mathbb{Z} \to \mathbb{Z}/n'\mathbb{Z}$ and $\nu_{n'} \colon \mathbb{Z} \to \mathbb{Z}/n'\mathbb{Z}$ we have $n\mathbb{Z} = \ker(\nu_n) \subseteq \ker(\nu_{n'}) = n'\mathbb{Z}$, hence by the homomorphism theorem there is an induced natural map $\nu_{n'}^n \colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n'\mathbb{Z} \colon \overline{z} \mapsto \overline{\overline{z}}$. The kernel of $\nu_{n'}^n$ is given as $\ker(\nu_{n'}^n) = \ker(\nu_{n'})/\ker(\nu_n) = n'\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, n' + n\mathbb{Z}, \ldots, (d-1)n' + n\mathbb{Z}\}$; in particular we have $|\ker(\nu_{n'}^n)| = d$.

By the above, $\overline{x}$ is a solution of $aX \equiv b \pmod{n}$ if and only if $\overline{\overline{x}}$ is a solution of $a'X \equiv b' \pmod{n'}$. We have $\gcd_+(a', n') = 1$, hence $\overline{\overline{a'}} \in (\mathbb{Z}/n'\mathbb{Z})^*$. Thus there is $\overline{\overline{c}} \in (\mathbb{Z}/n'\mathbb{Z})^*$ such that $\overline{\overline{a'c}} = \overline{\overline{1}} \in (\mathbb{Z}/n'\mathbb{Z})^*$, and we have $\overline{\overline{a'x}} = \overline{\overline{b'}} \in \mathbb{Z}/n'\mathbb{Z}$ if and only if $\overline{\overline{x}} = \overline{\overline{b'c}} \in \mathbb{Z}/n'\mathbb{Z}$. Thus the given linear congruence has a solution $\overline{x} := \overline{b'c} \in \mathbb{Z}/n\mathbb{Z}$, whose residue class $\nu^n_{n'}(\overline{x}) = \overline{\overline{x}} \in \mathbb{Z}/n'\mathbb{Z}$ is uniquely determined, hence the set of solutions is given as $\overline{x} + \ker(\nu^n_{n'}) = \{\overline{x}, \overline{x+n'}, \ldots, \overline{x+(d-1)n'}\} \subseteq \mathbb{Z}/n\mathbb{Z}$. ♯

In particular, we have $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$ if and only if we always have a solution, which is equivalent to saying that solutions, if existent, are unique.

Moreover, in general, the solutions can be found using the extended Euclidean algorithm: Computing $\gcd_+(a, n) = d$ yields Bézout coefficients $c, c' \in \mathbb{Z}$ such that $ac + nc' = d \in \mathbb{Z}$, hence letting $n' := \frac{n}{d}$ and $a' := \frac{a}{d}$ we have $a'c + n'c' = 1$, and thus we have $\overline{\overline{a'}}^{-1} = \overline{\overline{c}} \in \mathbb{Z}/n'\mathbb{Z}$. Hence the set of solutions is given as $\{\overline{x}, \overline{x+n'}, \ldots, \overline{x+(d-1)n'}\} \subseteq \mathbb{Z}/n\mathbb{Z}$, where $\overline{x} := \overline{b'c} \in \mathbb{Z}/n\mathbb{Z}$.

Example. We consider the linear congruence $35X \equiv b \pmod{126}$, where we may assume that $b \in \mathbb{Z}_{126}$. Hence we have $n = 126$ and $a = 35$, and there is a solution if and only if $d = 7 = \gcd_+(35, 126) \mid b$, that is $b \in \{0, 7, \ldots, 119\}$. In this case we have $n' = \frac{n}{d} = \frac{126}{7} = 18$ and $a' = \frac{a}{d} = \frac{35}{7} = 5$, yielding the linear congruence $5X \equiv b' \pmod{18}$, where $b' = \frac{b}{d} = \frac{b}{7} \in \mathbb{Z}_{18}$. From $d = 7 = 2 \cdot 126 - 7 \cdot 35 = 2n - 7a$, see (4.4), we get $1 = 2 \cdot 18 - 7 \cdot 5 = 2n' - 7a'$, hence we have $\overline{\overline{5}}^{-1} = -\overline{\overline{7}} = \overline{\overline{11}} \in \mathbb{Z}/18\mathbb{Z}$. This yields $\overline{\overline{x}} = \overline{\overline{11b'}} \in \mathbb{Z}/18\mathbb{Z}$. Thus the set of solutions is given as $\{\overline{11b'}, \overline{11b'+18}, \ldots, \overline{11b'+108}\} \subseteq \mathbb{Z}/126\mathbb{Z}$.

(8.2) Simultaneous linear congruences. Let $n_1, \ldots, n_k \in \mathbb{N}$, for some $k \in \mathbb{N}$, and $b_1, \ldots, b_k \in \mathbb{Z}$. We wonder when the system of linear congruences $X \equiv b_i \pmod{n_i}$, for all $i \in \{1, \ldots, k\}$, has a solution, and how these look like.

To this end, let $I_i := n_i\mathbb{Z} \trianglelefteq \mathbb{Z}$ and $\bigoplus_{i=1}^k \mathbb{Z}/I_i$ be the **direct sum** of the quotient rings $\mathbb{Z}/I_i$, that is the Cartesian product of the sets $\mathbb{Z}/I_i$, which is a commutative ring again with respect to componentwise addition and multiplication. Then we have the natural map $\nu_{n_1,\ldots,n_k} \colon \mathbb{Z} \to \bigoplus_{i=1}^k \mathbb{Z}/I_i \colon x \mapsto [x + I_1, \ldots, x + I_k]$, for which we have $\ker(\nu_{n_1,\ldots,n_k}) = \bigcap_{i=1}^k I_i = \operatorname{lcm}(n_1, \ldots, n_k)_+\mathbb{Z} \trianglelefteq \mathbb{Z}$. By the homomorphism theorem, $\nu_{n_1,\ldots,n_k}$ induces a ring isomorphism $\mathbb{Z}/\ker(\nu_{n_1,\ldots,n_k}) \to \operatorname{im}(\nu_{n_1,\ldots,n_k})$, where the latter is described as follows:

Theorem: Generalised Chinese remainder theorem. Let $I_{ij} := I_i + I_j = n_i\mathbb{Z} + n_j\mathbb{Z} = \gcd_+(n_i, n_j)\mathbb{Z}$, for $i < j \in \{1, \ldots, k\}$. Then we have

$$\operatorname{im}(\nu_{n_1,\ldots,n_k}) = \{[\overline{b}_1, \ldots, \overline{b}_k] \in \bigoplus_{i=1}^k \mathbb{Z}/I_i; b_i + I_{ij} = b_j + I_{ij} \in \mathbb{Z}/I_{ij} \text{ for all } i < j\}.$$

Proof. Let $R \subseteq \bigoplus_{i=1}^k \mathbb{Z}/I_i$ denote the right hand side, where since $I_i, I_j \subseteq I_{ij}$ the defining equations for R are indeed well-defined. By the natural map $\nu_{I_{ij}}^{I_i} : \mathbb{Z}/I_i \to \mathbb{Z}/I_{ij}$, for $x \in \mathbb{Z}$ we get $\nu_{I_{ij}}^{I_i}(x + I_i) = x + I_{ij} = \nu_{I_{ij}}^{I_j}(x + I_j)$. Hence we have $\mathrm{im}(\nu) \subseteq R$. For the converse, we first consider the case $k = 2$:

Writing $n, n' \in \mathbb{N}$ and $I := n\mathbb{Z} + n'\mathbb{Z}$ for simplicity, we have $R = \{[\overline{b}, \overline{b'}] \in \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n'\mathbb{Z}; \overline{b} + I = \overline{b'} + I \in \mathbb{Z}/I\}$. Letting $d := \gcd_+(n, n')$, there are Bézout coefficients $s, t \in \mathbb{Z}$ such that $d = sn + tn'$. Now for $[\overline{b}, \overline{b'}] \in R$ we have $b' - b \in I = d\mathbb{Z}$, thus there is $k \in \mathbb{Z}$ such that $b' - b = kd = ksn + ktn'$, hence $x := b + ksn = b' - ktn' \in \mathbb{Z}$ fulfills $\overline{x} = \overline{b + ksn} = \overline{b} \in \mathbb{Z}/n\mathbb{Z}$ and $\overline{x} = \overline{b' - ktn'} = \overline{b'} \in \mathbb{Z}/n'\mathbb{Z}$, showing that $\nu_{n,n'}(x) = [\overline{b}, \overline{b'}]$. Hence we conclude that $\mathrm{im}(\nu_{n,n'}) = R$, settling this case.

Next, for $k \geq 2$ we have the following relation $\gcd_+(\mathrm{lcm}_+(n_1, \ldots, n_{k-1}), n_k) = \mathrm{lcm}_+(\gcd_+(n_1, n_k), \ldots, \gcd_+(n_{k-1}, n_k))$: Since these numbers are determined prime-by-prime, we may assume that $n_i = p^{\alpha_i}$, for some $p \in \mathcal{P}$ and $\alpha_i \in \mathbb{N}_0$; then in terms of the multiplicities $\alpha_i \in \mathbb{N}_0$ the left hand side is translated into $\min\{\max\{\alpha_1, \ldots, \alpha_{k-1}\}, \alpha_k\}$, which is α_k if $\alpha_i \geq \alpha_k$ for some $i \in \{1, \ldots, k-1\}$, and otherwise is $\max\{\alpha_1, \ldots, \alpha_{k-1}\}$; the latter in turn equals $\max\{\min\{\alpha_1, \alpha_k\}, \ldots, \min\{\alpha_{k-1}, \alpha_k\}\}$, representing the right hand side.

Now we proceed by induction on $k \in \mathbb{N}$, where the case $k = 1$ is trivial. Hence let $k \geq 2$, and let $[\overline{b}_1, \ldots, \overline{b}_k] \in R$. Letting $J_{k-1} := \bigcap_{i=1}^{k-1} I_i$, the above relation between greatest common divisors and lowest common multiples translates into $J_{k-1} + I_k = \bigcap_{i=1}^{k-1} I_{ik} \trianglelefteq \mathbb{Z}$. By induction we may assume that there is $\overline{x} \in \mathbb{Z}/J_{k-1}$ such that $x + I_i = b_i + I_i \in \mathbb{Z}/I_i$, for $i \in \{1, \ldots, k-1\}$. We have $x + I_{ik} = b_i + I_{ik} = b_k + I_{ik} \in \mathbb{Z}/I_{ik}$, for all $i \in \{1, \ldots, k-1\}$, entailing $x - b_k \in \bigcap_{i=1}^{k-1} I_{ik} = J_{k-1} + I_k$, or equivalently $x + J_{k-1} + I_k = b_k + J_{k-1} + I_k \in \mathbb{Z}/(J_{k-1} + I_k)$. Thus the two-moduli case yields the existence of $\overline{y} \in \mathbb{Z}/(J_{k-1} \cap I_k)$ such that $y + J_{k-1} = x + J_{k-1} \in \mathbb{Z}/J_{k-1}$ and $y + I_k = b_k + I_k \in \mathbb{Z}/I_k$. ♯

Corollary: Chinese remainder theorem. Let now $n_1, \ldots, n_k$ be pairwise coprime, that is $\gcd_+(n_i, n_j) = 1$, or equivalently $I_{ij} = I_i + I_j = \mathbb{Z}$, for all $i \neq j \in \{1, \ldots, k\}$. Then we have

i) $\mathrm{lcm}(n_1, \ldots, n_k)_+ = \prod_{i=1}^k n_i$, that is $\ker(\nu_{n_1,\ldots,n_k}) = \bigcap_{i=1}^k I_i = \prod_{i=1}^k I_i$, and

ii) $\nu_{n_1,\ldots,n_k}$ is surjective, that is $\mathrm{im}(\nu_{n_1,\ldots,n_k}) = \bigoplus_{i=1}^k \mathbb{Z}/I_i$.

Thus $\nu_{n_1,\ldots,n_k}$ induces a ring isomorphism $\mathbb{Z}/(\prod_{i=1}^k n_i)\mathbb{Z} \to \bigoplus_{i=1}^k \mathbb{Z}/n_i\mathbb{Z}$. ♯

In other words, the system of linear congruences $X \equiv b_i \pmod{n_i}$, for all $i \in \{1, \ldots, k\}$, has a solution if and only if $b_i \equiv b_j \pmod{\gcd_+(n_i, n_i)}$, for all $i < j \in \{1, \ldots, k\}$, and in this case the solution is unique in $\mathbb{Z}/\mathrm{lcm}_+(n_1, \ldots, n_k)\mathbb{Z}$. In particular, if the moduli $n_1, \ldots, n_k$ are pairwise coprime, then the system always has a solution, which is unique in $\mathbb{Z}/(\prod_{i=1}^k n_i)\mathbb{Z}$.

Reduction to the coprime case. A single linear congruence can always be replaced by a system of linear congruences with respect to prime power moduli; but note that to do so the modulus in question has to be factorised first: If $n = \prod_{i=1}^{k} p_i^{a_i} \in \mathbb{N}$, where $p_i \in \mathcal{P}$ are pairwise distinct primes and $a_i \geq 0$, for $i \in \{1, \ldots, k\}$, then $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ solves the linear congruence $X \equiv b \pmod{n}$ if and only if $\overline{x} \in \mathbb{Z}/p_i^{a_i}\mathbb{Z}$ solves the linear congruence $X \equiv b \pmod{p_i^{a_i}}$, for all $i \in \{1, \ldots, k\}$. Hence the number of solutions modulo $n\mathbb{Z}$ is given as the product of the number of solutions modulo $p_i^{a_i}\mathbb{Z}$, for $i \in \{1, \ldots, k\}$.

Assuming this, since the solvability conditions are always fulfilled between coprime moduli, the remaining checks can be done prime-by-prime. Given $p \in \mathcal{P}$, applying the the natural maps $\nu_{p^{k-1}}^{p^k}$, where $k \geq 2$, shows that if the conditions are fulfilled for p-powers, then only the linear congruence with respect to the largest p-power occurring is irredundant. Hence this reduces the problem of finding the solutions of a given system of linear congruences to finding a solution of a system of linear congruences with respect to pairwise coprime moduli.

(8.3) Solving simultaneous linear congruences. The results of (8.2) are made constructive using the extended Euclidean algorithm as follows:

a) In the general case, the **Newton method** runs as follows: Let $l_0 := 1$ and $l_i := \mathrm{lcm}_+(n_1, \ldots, n_i) = \mathrm{lcm}_+(n_i, l_{i-1})$, for $i \in \{1, \ldots, k\}$. Then let $x_1 := b_1 \in \mathbb{Z}$, and for $i \in \{2, \ldots, k\}$ let successively $x_i \in \mathbb{Z}$ be a solution of the system

$$X \equiv b_i \pmod{n_i} \quad \text{and} \quad X \equiv x_{i-1} \pmod{l_{i-1}},$$

which, letting $d_i := \gcd_+(n_i, l_{i-1})$ and $s_i, t_i \in \mathbb{Z}$ being Bézout coefficients such that $d_i = s_i n_i + t_i l_{i-1}$, is found as $x_i := b_i + \frac{x_{i-1} - b_i}{d_i} \cdot s_i n_i \in \mathbb{Z}$. Note that the solvability conditions translate precisely into the conditions $d_i \mid (x_{i-1} - b_i)$, for $i \in \{1, \ldots, k\}$, and that x_i is unique modulo $l_i\mathbb{Z}$. This yields the following:

- $l_0 \leftarrow 1$, $l_1 \leftarrow n_1$, $x_1 \leftarrow b_1 \bmod l_1$
- for $i \in [2, \ldots, k]$ do
  - $l_i \leftarrow (n_i l_{i-1})$ div $\gcd_+(n_i, l_{i-1})$ # $\mathrm{lcm}_+(n_i, l_{i-1})$
  - $[d_i; s_i, t_i] \leftarrow \mathsf{EEA}(n_i, l_{i-1})$ # $d_i = \gcd_+(n_i, l_{i-1}) = s_i n_i + t_i l_{i-1}$
  - if $((x_{i-1} - b_i) \bmod d_i) > 0$ then # no solution
    - return fail
  - $x_i \leftarrow (b_i + (x_{i-1} - b_i) \cdot ((s_i n_i) \text{ div } d_i)) \bmod l_i$
- return x_k

b) If the moduli $n_1, \ldots, n_k$ are pairwise coprime, there also is the more direct **Lagrange method**: For $i \in \{1, \ldots, k\}$ let $m_i := \prod_{j \neq i} n_i$. Then we have $\gcd_+(m_i, n_i) = 1$, hence there are Bézout coefficients $s_i, t_i \in \mathbb{Z}$ such that $s_i m_i + t_i n_i = 1$. Thus we have $\overline{s_i m_i} = \overline{1 - t_i n_i} = \overline{1} \in \mathbb{Z}/n_i\mathbb{Z}$, and $\overline{s_i m_i} = \overline{s_i \cdot \prod_{j \neq i} n_i} = \overline{0} \in \mathbb{Z}/n_j\mathbb{Z}$ for all $i \neq j \in \{1, \ldots, k\}$. Hence for $x := \sum_{i=1}^{k} b_i \cdot s_i m_i \in \mathbb{Z}$ we have $\overline{x} = \sum_{j=1}^{k} \overline{b_j s_j m_j} = \overline{b_i s_i m_i} = \overline{b_i} \in \mathbb{Z}/n_i\mathbb{Z}$, for $i \in \{1, \ldots, k\}$. Thus x solves the given system of linear congruences, and is unique modulo $(\prod_{i=1}^{k} n_i)\mathbb{Z}$.

Example. The system of linear congruences

$$X \equiv 1 \pmod{21} \quad \text{and} \quad X \equiv 2 \pmod{45}$$

does not have a solution: We have $\gcd_+(21, 45) = 3$, but $1 \not\equiv 2 \pmod 3$.

Alternatively, we may more explicitly argue as follows: The linear congruence $X \equiv 1 \pmod{21}$ is equivalent to the system of linear congruences $X \equiv 1 \pmod 3$ and $X \equiv 1 \pmod 7$, while the linear congruence $X \equiv 2 \pmod{45}$ is equivalent to the system of linear congruences $X \equiv 2 \pmod 9$ and $X \equiv 2 \pmod 5$; but now considering 3-power moduli we observe that $x \equiv 1 \pmod 9$ entails $x \equiv 1 \pmod 3$, contradicting the condition $x \equiv 2 \pmod 3$. ♯

Example. The following example is taken from [2, Ch.8.1]: *Six professors begin courses of lectures on Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday, and announce their intentions of lecturing at intervals of two, three, four, one, six, and five days respectively. The regulations of the university forbid Sunday lectures (so that a Sunday lecture must be omitted). When first will all six professors find themselves compelled to omit a lecture?*

If $x \in \mathbb{N}$ is the day sought for, where $x = 1$ is the first Monday, this leads to the following system of linear congruences:

$$X \equiv 1 \pmod 2, \quad X \equiv 2 \pmod 3, \quad X \equiv 3 \pmod 4, \quad X \equiv 4 \pmod 1,$$
$$X \equiv 5 \pmod 6, \quad X \equiv 6 \pmod 5, \quad X \equiv 0 \pmod 7.$$

To check the solvability conditions, we only have to consider pairs of non-coprime moduli, which yields $\gcd(2, 4)_+ = 2$ where $1 \equiv 3 \pmod 2$, and $\gcd(2, 6)_+ = 2$ where $1 \equiv 5 \pmod 2$, as well as $\gcd(3, 6)_+ = 3$ where $2 \equiv 5 \pmod 3$, and $\gcd(4, 6)_+ = 2$ where $3 \equiv 5 \pmod 2$. Hence the system has a solution, which is unique modulo $\operatorname{lcm}_+(2, 3, 4, 1, 6, 5, 7) = 2^2 \cdot 3 \cdot 5 \cdot 7 = 420$.

To find the solutions using the recursive method, we proceed as shown in Table 6; hence the smallest non-negative solution looked for is given as $x = x_7 = 371$. Alternatively, we may transform the system suitably, in order to solve an equivalent system with pairwise coprime moduli:

The linear congruence $X \equiv 4 \pmod 1$ is always fulfilled, hence redundant. The linear congruence $X \equiv 5 \pmod 6$ is equivalent to the system of linear congruences $X \equiv 5 \equiv 1 \pmod 2$ and $X \equiv 5 \equiv 2 \pmod 3$. The linear congruence $X \equiv 3 \pmod 4$ implies $X \equiv 3 \equiv 1 \pmod 2$, hence the latter is redundant. Thus we are left with the equivalent system of linear congruences

$$X \equiv 2 \pmod 3, \quad X \equiv 3 \pmod 4, \quad X \equiv 1 \pmod 5, \quad X \equiv 0 \pmod 7.$$

Table 6: Generalised Chinese remainder theorem.

i	n_i	l_i	$d_i = s_i n_i + t_i l_{i-1}$	$\frac{s_i n_i}{d_i}$	b_i	$x_i \bmod l_i$
1	2	2			1	1
2	3	6	$1 = 1 \cdot 3 - 1 \cdot 2$	3	2	5
3	4	12	$2 = -1 \cdot 4 + 1 \cdot 6$	-2	3	11
4	1	12	$1 = 1 \cdot 1 + 0 \cdot 12$	1	4	11
5	6	12	$6 = 1 \cdot 6 + 0 \cdot 12$	1	5	11
6	5	60	$1 = 5 \cdot 5 - 2 \cdot 12$	25	6	11
7	7	420	$1 = -17 \cdot 7 + 2 \cdot 60$	-119	0	371

Now the moduli are pairwise coprime (and prime powers), and we get:

i	n_i	m_i	$1 = s_i m_i + t_i n_i$	$s_i m_i$	b_i
1	3	140	$1 = -1 \cdot 140 + 47 \cdot 3$	-140	2
2	4	105	$1 = 1 \cdot 105 - 26 \cdot 4$	105	3
3	5	84	$1 = -1 \cdot 84 + 17 \cdot 5$	-84	1
4	7	60	$1 = 2 \cdot 60 - 17 \cdot 7$	120	0

This yields the solution $x := -2 \cdot 140 + 3 \cdot 105 - 1 \cdot 84 + 0 \cdot 120 = -49 \in \mathbb{Z}$. Hence the smallest non-negative solution looked for is given as $(x \bmod 420) = 371$. ♯

9 Polynomial congruences

(9.1) Polynomial congruences. Given $n \in \mathbb{N}$ and a polynomial $f \in \mathbb{Z}[X]$, we wonder when the **polynomial congruence** $f(X) \equiv 0 \pmod{n}$ has a solution.

As in the special case of linear congruences, this question can be reduced to prime power moduli: If $n = \prod_{i=1}^{k} p_i^{a_i} \in \mathbb{N}$, where $p_i \in \mathcal{P}$ are pairwise distinct primes and $a_i \geq 0$, for $i \in \{1, \ldots, k\}$, then by the Chinese remainder theorem $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ is a solution of the polynomial congruence $f(X) \equiv b \pmod{n}$ if and only if $\overline{x} \in \mathbb{Z}/p_i^{a_i}\mathbb{Z}$ is a solution of the polynomial congruence $f(X) \equiv b \pmod{p_i^{a_i}}$, for all $i \in \{1, \ldots, k\}$. Hence the number of solutions modulo $n\mathbb{Z}$ is given as the product of the number of solutions modulo $p_i^{a_i}\mathbb{Z}$, for $i \in \{1, \ldots, k\}$.

But in contrast to the case of systems of linear congruences, where for any prime $p \in \mathcal{P}$ only a finite number of consistency checks are needed to decide solvability, and then the solution is unique modulo the largest p-power occurring, the situation here is more complicated:

Applying the natural map $\nu_{p^l}^{p^k}$, where $l \leq k$, to a solution of the polynomial congruence $f(X) \equiv 0 \pmod{p^k}$ yields a solution of the polynomial congruence $f(X) \equiv 0 \pmod{p^l}$. But now the question is whether conversely a solution modulo $p^l\mathbb{Z}$ can be lifted to a solution modulo $p^k\mathbb{Z}$, and if so how many lifts there are. The answer will turn out to be positive, so that in conclusion solving a given

polynomial congruence modulo $n\mathbb{Z}$ reduces to solving polynomial congruences modulo $p\mathbb{Z}$, for various $p \in \mathcal{P}$.

More precisely, let $\overline{f} \in \mathbb{Z}/p\mathbb{Z}[X]$ be the polyonomial obtained by applying the natural map ν_p to the coefficients of the given polynomial $f \in \mathbb{Z}[X]$. Then solving the polynomial congruence $f(X) \equiv 0 \pmod{p}$ is equivalent to finding the roots of $\overline{f}$ in the field $\mathbb{Z}/p\mathbb{Z}$. Now $\mathbb{Z}/p\mathbb{Z}[X]$ is Euclidean, with degree map given by polynomial degree, and quotient and remainder given by polynomial division, hence in particular is factorial. (We take these facts for granted here, but they are not too difficult to show anyway.) This implies that the number of roots $\overline{a}$ of $\overline{f} \neq \overline{0}$, that is the number of (irreducible monic) divisors $X - \overline{a}$ of $\overline{f}$, is bounded above by the degree of $\overline{f}$; the polynomial $\overline{f} = \overline{0}$ has all elements of $\mathbb{Z}/p\mathbb{Z}$ as roots. (We will not discuss here how root finding, or more generally polynomial factorisation, can be done algorithmically and efficiently.)

Example. Let $n := 15 = 3 \cdot 5$ and $f := X^2 - 1 \in \mathbb{Z}[X]$. To find the solutions of the polynomial congruence $f(X) \equiv 0 \pmod{15}$, that is the square roots of $\overline{1} \in \mathbb{Z}/15\mathbb{Z}$, we first determine the solutions of the polynomial congruences $f(X) \equiv 0 \pmod{3}$ and $f(X) \equiv 0 \pmod{3}$, respectively:

Given $p \in \mathcal{P}$, the polynomial $\overline{f} = X^2 - \overline{1} \in \mathbb{Z}/p\mathbb{Z}[X]$ has precisely the roots $\pm\overline{1} \in \mathbb{Z}/p\mathbb{Z}$. Hence we let $\overline{a}_\pm := \pm\overline{1} \in \mathbb{Z}/3\mathbb{Z}$ and $\overline{b}_\pm := \pm\overline{1} \in \mathbb{Z}/5\mathbb{Z}$. Thus $1 = \gcd + (5, 3) = -1 \cdot 5 + 2 \cdot 3$ yields the four solutions $-5a_\pm + 6b_\pm \pmod{15}$, that is $\{\pm\overline{1}, \pm\overline{4}\} \subseteq \mathbb{Z}/15\mathbb{Z}$, of the polynomial congruence $X^2 \equiv 1 \pmod{15}$.

(9.2) Polynomial congruences modulo prime powers. We are now going to describe under which circumstances a solution of a polynomial congruence modulo $p^k\mathbb{Z}$, where $p \in \mathcal{P}$ and $k \in \mathbb{N}$, can be lifted to a solution modulo $p^l\mathbb{Z}$, where $l > k$. To do so, need a few preparations first:

Let $\frac{\partial}{\partial X} \colon \mathbb{Z}[X] \to \mathbb{Z}[X] \colon f \mapsto f^{(1)}$ be the **formal derivative**, that is the $\mathbb{Z}$-linear map given by $1 \mapsto 0$, and $X^i \mapsto iX^{i-1}$ for $i \in \mathbb{N}$. Letting $f^{(0)} := f \in \mathbb{Z}[X]$, by induction on $k \in \mathbb{N}$ we get its k-th formal derivative $f^{(k)} := (f^{(k-1)})^{(1)} \in \mathbb{Z}[X]$. Hence we have $f^{(k)}(X^i) = 0$ for $i \in \{0, \ldots, k-1\}$, and $f^{(k)}(X^i) = \frac{i!}{(i-k)!} X^{i-k} = k!\binom{i}{k} X^{i-k}$ for $i \geq k$. Thus we may let $f^{[k]} := \frac{1}{k!} f^{(k)} \in \mathbb{Z}[X]$ be the k-th **Hasse-Teichmüller derivative** of f.

Now, for $i \in \mathbb{N}_0$, binomial expansion yields $(X + Y)^i = \sum_{k=0}^{i} \binom{i}{k} Y^{i-k} X^k \in \mathbb{Z}[X, Y]$, where we have $\binom{i}{k} Y^{i-k} = (X^i)^{[k]}(Y)$, that is the evaluation of the k-th Hasse-Teichmüller derivative of $X^i \in \mathbb{Z}[X]$ at Y. Thus for any $f \in \mathbb{Z}[X]$ we get $f(Y + X) = \sum_{k \geq 0} f^{[k]}(Y) \cdot X^k \in \mathbb{Z}[X, Y]$. In particular, evaluating at $[X - a, a]$ for $a \in \mathbb{Z}$, we get the **Taylor expansion** $f(X) = \sum_{k \geq 0} f^{[k]}(a) \cdot (X - a)^k \in \mathbb{Z}[X]$, and evaluating at $[b, a]$ for $a, b \in \mathbb{Z}$, yields $f(a + b) = \sum_{k \geq 0} f^{[k]}(a) \cdot b^k \in \mathbb{Z}$.

Theorem: Hensel's Lemma. Let $p \in \mathcal{P}$, let $f \in \mathbb{Z}[X]$, and let $a \in \mathbb{Z}$ such that $f(a) \equiv 0 \pmod{p^k}$ for some $k \in \mathbb{N}$. Moreover, let $l \in \{1, \ldots, k\}$ and

$m \in \{0, \ldots, l\}$ such that $p^m = \gcd_+(f^{(1)}(a), p^l)$. Then precisely one of the following cases occurs:

i) If $m = 0$, that is $f^{(1)}(a) \not\equiv 0 \pmod{p}$, then there is a unique $\overline{\widehat{a}} \in \mathbb{Z}/p^{k+l}\mathbb{Z}$ such that $\widehat{a} \equiv a \pmod{p^k}$ and $f(\widehat{a}) \equiv 0 \pmod{p^{k+l}}$.

ii) If $m > 0$ and $f(a) \not\equiv 0 \pmod{p^{k+m}}$, then there is no element $\overline{\widehat{a}} \in \mathbb{Z}/p^{k+l}\mathbb{Z}$ such that $\widehat{a} \equiv a \pmod{p^k}$ and $f(\widehat{a}) \equiv 0 \pmod{p^{k+l}}$.

iii) If $m > 0$ and $f(a) \equiv 0 \pmod{p^{k+m}}$, then there precisely p^m elements $\overline{\widehat{a}} \in \mathbb{Z}/p^{k+l}\mathbb{Z}$ such that $\widehat{a} \equiv a \pmod{p^k}$ and $f(\widehat{a}) \equiv 0 \pmod{p^{k+l}}$.

Moreover, for any $\widehat{a}$ ocurring above we have $\gcd_+(f^{(1)}(\widehat{a}), p^l) = p^m$.

Proof. We consider $x := a + yp^k \in \mathbb{Z}$ for $y \in \mathbb{Z}$. Then Taylor expansion yields $f(x) = f(a + yp^k) = \sum_{j \geq 0} f^{[j]}(a) \cdot (yp^k)^j = f(a) + f^{(1)}(a) \cdot yp^k + y^2 p^{2k} z \in \mathbb{Z}$, where $z := \sum_{j \geq 2} f^{[j]}(a) \cdot (yp^k)^{j-2} \in \mathbb{Z}$. Hence we have $f(x) \equiv f(a) + f^{(1)}(a) \cdot yp^k \pmod{p^{k+l}}$. Moreover, there is $b \in \mathbb{Z}$ such that $f(a) = bp^k$. Hence we have $f(a) + f^{(1)}(a) \cdot yp^k = p^k \cdot (b + f^{(1)}(a) \cdot y) \in \mathbb{Z}$. Thus we have $f(x) \equiv 0 \pmod{p^{k+l}}$ if and only if $b + f^{(1)}(a) \cdot y \equiv 0 \pmod{p^l}$. Hence we are led to consider the latter linear congruence:

If $m = 0$, that is $\overline{f^{(1)}(a)} \in (\mathbb{Z}/p^l\mathbb{Z})^*$, then the linear congruence $f^{(1)}(a) \cdot Y + b \equiv 0 \pmod{p^l}$ has the unique solution $\overline{y} := -\overline{b} \cdot \overline{f^{(1)}(a)}^{-1} \in \mathbb{Z}/p^l\mathbb{Z}$. Hence $\widehat{a} := a + yp^k \in \mathbb{Z}$ is the unique lift modulo $p^{k+l}\mathbb{Z}$, implying i).

If $m > 0$, then the linear congruence $f^{(1)}(a) \cdot Y + b \equiv 0 \pmod{p^l}$ has a solution if and only if $b \equiv 0 \pmod{p^m}$, or equivalently $f(a) \equiv 0 \pmod{p^{k+m}}$. Hence, if $b \not\equiv 0 \pmod{p^m}$ then the latter linear congruence does not have a solution, implying ii), while if $b \equiv 0 \pmod{p^m}$ then it has precisely p^m solutions.

Finally, since $\widehat{a} \equiv a \pmod{p^k}$ we have $f^{(1)}(\widehat{a}) \equiv f^{(1)}(a) \pmod{p^l}$, implying that $\gcd_+(f^{(1)}(\widehat{a}), p^l) = \gcd_+(f^{(1)}(a), p^l) = p^m$. ♯

The typical cases are 'simple root' lifting $m = 0$, where $l = 0$ or $l = k$, and the exceptional lifting $m = l = 1$.

Remark. Hensel lifting is a 'p-adic' analogue of the (quadratically convergent) **Newton iteration** to find zeroes of real-valued functions: Let $f \in C^2(I)$ be a two-fold continuously differentiable function, where $I \subseteq \mathbb{R}$ is an open interval, such that $f(\xi) = 0$ for some $\xi \in I$, and $f^{(1)} > 0$ and $f^{(2)} < 0$ on I, where $f^{(1)} := \frac{\partial f}{\partial x}$ and $f^{(2)} := \frac{\partial f^{(1)}}{\partial x}$ are the first and second derivatives of f. Choosing $x_0 \in I$, and letting $x_{i+1} := x_i - \frac{f(x_i)}{f^{(1)}(x_i)}$, for $i \in \mathbb{N}_0$, it can be shown that the x_i are well-defined, and that $\lim_{i \to \infty} x_i = \xi$ converges (quadratically). This is motivated by the idea of replacing f by the linear part l of its Taylor expansion: The tangent line to the graph of f at $[x_i, f(x_i)]$ is given as $l(x) := f(x_i) + f^{(1)}(x_i) \cdot (x - x_i)$, for $x \in \mathbb{R}$, where $l(x) = 0$ if and only if $x := x_i - \frac{f(x_i)}{f^{(1)}(x_i)}$.

Example. Let $f := X^2 - 2 \in \mathbb{Z}[X]$, hence $f^{(1)} = 2X \in \mathbb{Z}[X]$. We consider the polynomial congruence $f(X) \equiv 0 \pmod{p^k}$ for various $p \in \mathcal{P}$ and $k \in \mathbb{N}$:

Let $p := 7$. Then we have $\overline{f} = X^2 - \overline{2} = (X - \overline{3})(X + \overline{3}) \in \mathbb{Z}/7\mathbb{Z}[X]$ and $\overline{f^{(1)}} = \overline{2}X \in \mathbb{Z}/7\mathbb{Z}[X]$. Hence we may let $a := 3$. Then we have $f(\pm a) \equiv 0 \pmod 7$ and $f^{(1)}(\pm a) \equiv \mp 1 \pmod 7$, thus $m = 0$. Running Hensel lifting on a, we get the unique solution of the polynomial congruence $f(X) \equiv 0 \pmod{7^k}$, for $k \in \mathbb{N}$, being congruent to a modulo $7\mathbb{Z}$, as indicated in Table 7, for $l = 1$ and $l = k$, respectively; we use numerically smallest residues in $\mathbb{Z}/7^k\mathbb{Z}$, and $\bar{}$ denotes elements of $\mathbb{Z}/7\mathbb{Z}$. Since negating respects solutions modulo $7^k\mathbb{Z}$, for $k \in \mathbb{N}$, Hensel lifting on $-a$ runs in parallel with opposite signs.

For $p := 5$ we have $\{\overline{a}^2 \in \mathbb{Z}/5\mathbb{Z}; \overline{a} \in \mathbb{Z}/5\mathbb{Z}\} = \{\overline{0}, \pm\overline{1}\}$, hence $\overline{f} = X^2 - \overline{2} \in \mathbb{Z}/5\mathbb{Z}[X]$ does not have a root in $\mathbb{Z}/5\mathbb{Z}[X]$, thus neither of the polynomial congruences $f(X) \equiv 0 \pmod{5^k}$, where $k \in \mathbb{N}$, has a solution. Similarly, for $p := 3$ we have $\{\overline{a}^2 \in \mathbb{Z}/5\mathbb{Z}; \overline{a} \in \mathbb{Z}/5\mathbb{Z}\} = \{\overline{0}, \overline{1}\}$, hence $\overline{f} = X^2 - \overline{2} \in \mathbb{Z}/3\mathbb{Z}[X]$ does not have a root in $\mathbb{Z}/3\mathbb{Z}[X]$, thus neither of the polynomial congruences $f(X) \equiv 0 \pmod{3^k}$, where $k \in \mathbb{N}$, has a solution.

Let $p := 2$. Then we have $\overline{f} = X^2 \in \mathbb{Z}/2\mathbb{Z}[X]$ and $\overline{f^{(1)}} = \overline{0} \in \mathbb{Z}/2\mathbb{Z}[X]$. Hence we may let $a := 0$. Then we have $f(a) \equiv 0 \pmod 2$ and $f^{(1)}(a) \equiv 0 \pmod 2$, hence we have $m = l = k = 1$. Since $f(a) \equiv -2 \not\equiv 0 \pmod{2^2}$, the polynomial congruences $f(X) \equiv 0 \pmod{2^k}$, for $k \geq 2$, do not have a solution. (Indeed, a square in $\mathbb{Z}$ is odd or divisible by 4, thus is incongruent to 2 modulo $4\mathbb{Z}$.) ♯

IV Residues

10 Prime residue classes

(10.1) Euler's totient function. A map $\alpha\colon \mathbb{N} \to \mathbb{C}$ is also called a **number theoretic function**. A number theoretic function is called **multiplicative** if for all $m, n \in \mathbb{N}$ such that $\gcd_+(m, n) = 1$ we have $\alpha(mn) = \alpha(m)\alpha(n)$. In this case, if $\alpha \neq 0$ then we have $\alpha(1) = 1$, and using factorisations α is uniquely determined by its values on prime powers. Properties of number theoretic functions are of general interest. Here is a most prominent example:

Recall that for $n \in \mathbb{N}$ the group of prime residue classes equals $(\mathbb{Z}/n\mathbb{Z})^* = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z}; \gcd_+(a, n) = 1\}$. This gives rise to **Euler's totient function** $\varphi\colon \mathbb{N} \to \mathbb{N}\colon n \mapsto |(\mathbb{Z}/n\mathbb{Z})^*|$. In particular, we have $\varphi(1) = 1$, and n is a prime if and only if $\varphi(n) = n - 1$.

Proposition. a) Euler's totient function φ is multiplicative.

b) For $p \in \mathcal{P}$ and $k \in \mathbb{N}$ we have $\varphi(p^k) = (p-1)\cdot p^{k-1}$; in particular $\varphi(p) = p-1$.

Proof. a) For $m, n \in \mathbb{N}$ such that $\gcd_+(m, n) = 1$, by the Chinese remainder theorem we have the ring isomorphism $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}\colon a +$

Table 7: Hensel lifting.

k	a	$\overline{b}$	$\overline{y}$
1	3	1	1
2	10	2	2
3	108	−1	−1
4	−235	2	2
5	4567	2	2
6	38181	1	1
7	155830	2	2
8	1802916	−3	−3
9	−15491487	0	0
1	−15491487	0	0
11	−15491487	3	3
12	5916488742	1	1
13	19757775943	1	1
14	116646786350	0	0
15	116646786350	2	2
16	9611769806236		

k	a	b	$f^{(1)}(a)^{-1}$	y
1	3	1	−1	1
2	10	2	−22	−5
4	−235	23	−659	751
8	1802916	563854	450729	1667320
16	9611769806236	2779957025294	2402942451559	−6397056082836

$mn\mathbb{Z} \mapsto [a+n\mathbb{Z}, a+m\mathbb{Z}]$. Hence this induces a group isomorphism $(\mathbb{Z}/mn\mathbb{Z})^* \cong (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$, where the right hand side becomes a group with respect to componentwise multiplication. Thus we infer $\varphi(mn) = \varphi(m)\varphi(n)$.

b) For $k \in \mathbb{N}$ we have $(\mathbb{Z}/p^k\mathbb{Z})^* = \{\overline{x} \in \mathbb{Z}/p^k\mathbb{Z}; \gcd_+(x, p^k) = 1\} = \{\overline{x} \in \mathbb{Z}/p^k\mathbb{Z}; \gcd_+(x, p) = 1\}$ which is in bijection with $\{x \in \mathbb{Z}_{p^k}; \gcd_+(x, p) = 1\} = \{x \in \mathbb{Z}_{p^k}; p \nmid x\} = \mathbb{Z}_{p^k} \setminus \{x \in \mathbb{Z}_{p^k}; p \mid x\} = \mathbb{Z}_{p^k} \setminus \{py \in \mathbb{Z}_{p^k}; y \in \mathbb{Z}_{p^{k-1}}\}$. This entails $\varphi(p^k) = |(\mathbb{Z}/p^k\mathbb{Z})^*| = |\mathbb{Z}_{p^k}| - |\mathbb{Z}_{p^{k-1}}| = p^k - p^{k-1} = (p-1) \cdot p^{k-1}$. ♯

This elucidates the cardinality of the finite group $(\mathbb{Z}/n\mathbb{Z})^*$. We now proceed to investigate into its group structure. By the above argument, we will be able to reduce to the case where n is a prime power. We need a few general preparations from finite group theory first:

(10.2) Cosets. Let G be a (multiplicative) group, and let $U \leq G$ be a subgroup. We consider the following relation $\sim_U$ on G: For elements $g, h \in G$ we

let $g \sim_U h$ if there is $u \in U$ such that $h = ug$. Then from $g = 1 \cdot g$ we infer that $\sim_U$ is reflexive; from $h = ug$ we get $g = u^{-1}h$, showing that $\sim_U$ is symmetric; and from $h = ug$ and $k = vh$, for $k \in G$ and $v \in U$, we get $k = vug$, implying that $\sim_U$ is transitive. Thus $\sim_U$ is an equivalence relation on G.

The equivalence class $Ug := \{ug \in G; u \in U\} \subseteq G$ of $g \in G$ is called the associated **(right) coset** of U in G. Let $U/G := \{Ug \subseteq G; g \in G\}$ be the set of all cosets. Hence choosing a **(right) transversal** $\mathcal{T} \subseteq G$ of U in G, that is a set of representatives of the equivalence classes, we have $G = \coprod_{t \in \mathcal{T}} Ut$; note that a transversal always exists by the Axiom of Choice.

Lagrange's Theorem. Let G be finite and $U \leq G$. For the associated **group orders** we have $|U| \mid |G|$.

Proof. For $g \in G$, the surjective map $U \to Ug\colon u \mapsto ug$ is injective as well, hence is a bijection: For $u, v \in U$ such that $ug = vg$ we get $u = ugg^{-1} = vgg^{-1} = v$. This implies that all cosets have the same cardinality $|U|$, which entails $|G| = |U| \cdot |\mathcal{T}|$; note that by assumption all cardinalities are finite. ♯

(10.3) Element orders. Let G be a group, and $g \in G$. Then $\langle g \rangle := \{g^k \in G; k \in \mathbb{Z}\} \leq G$ is the smallest subgroup of G containing g: Any subgroup of G containing g also encompasses $\langle g \rangle$; and $\langle g \rangle$ contains 1_G and is closed with respect to multiplication and taking inverses, thus indeed is a subgroup of G.

The subgroup $\langle g \rangle$ is called the subgroup of G **generated** by g. The number $|g| := |\langle g \rangle| \in \mathbb{N} \cup \{\infty\}$ is called the **order** of g. In particular, if G is finite, then $|g|$ is finite as well, and Lagrange's Theorem implies that $|g| \mid |G|$.

Proposition. For $g \in G$ let $I(g) := \{i \in \mathbb{Z}; g^i = 1\}$.

a) Then $I(g) \trianglelefteq \mathbb{Z}$ is an ideal, where we have $I(g) = \{0\}$ if and only if $|g| = \infty$. Moreover, $\mathbb{Z}/I(g) \to \langle g \rangle\colon \overline{k} \mapsto g^k$ is an isomorphism from the additive group $(\mathbb{Z}/I(g), +)$ to the multiplicative group $\langle g \rangle$.

b) If $|g|$ is finite, then we have $I(g) = |g|\mathbb{Z}$ and $\langle g \rangle = \{g^k \in G; k \in \mathbb{Z}_{|g|}\}$; in particular, we have $g^{|g|} = 1$, and thus if G is finite we infer $g^{|G|} = 1$.

Proof. a) We have $g^0 = 1 \in G$, and for $i, j \in I(g)$ we have $g^{-i} = (g^i)^{-1} = 1$ and $g^{i+j} = g^i g^j = 1$, showing that $I(g) \subseteq \mathbb{Z}$ is an additive subgroup; and for $k \in \mathbb{Z}$ we get $g^{ik} = (g^i)^k = 1$, showing that $I(g) \trianglelefteq \mathbb{Z}$ is an ideal. Now for $k, l \in \mathbb{Z}$ we have $g^k = g^l$ if and only if $g^{k-l} = 1$, that is $k - l \in I(g)$, or equivalently $\overline{k} = \overline{l} \in \mathbb{Z}/I(g)$. Hence the map $\mathbb{Z}/I(g) \to \langle g \rangle\colon \overline{k} \mapsto g^k$ is well-defined and a bijection, where from $\overline{k} + \overline{l} = \overline{k+l} \mapsto g^{k+l} = g^k g^l$ we infer that it is a homormorphism from $(\mathbb{Z}/I(g), +)$ to $\langle g \rangle$. In particular, we have $I(g) = \{0\}$ if and only if $|\mathbb{Z}/I(g)| = \infty$, that is $|g| = \infty$.

b) If $|g|$ is finite, then $\{0\} \neq I(g) = n\mathbb{Z} \trianglelefteq \mathbb{Z}$ is principal, where we may assume that $n \in \mathbb{N}$ is smallest such that $n \in I(g)$. From $n = |\mathbb{Z}/I(g)| = |\langle g\rangle| = |g|$ we get $I(g) = |g|\mathbb{Z}$. The last assertion follows from $|g| \mid |G|$. ♯

Corollary. a) Let $n := |g|$ be finite. Then for $k \in \mathbb{Z}$ we have $|g^k| = \frac{n}{\gcd_+(k,n)}$.

In particular, we have $|g^k| = n$, that is $\langle g^k\rangle = \langle g\rangle$, if and only if $\gcd_+(k,n) = 1$, in other words if and only if $\overline{k} \in (\mathbb{Z}/n\mathbb{Z})^*$.

b) Let $g^n = 1$ for some $n \in \mathbb{N}$, and let $p_1, \ldots, p_r \in \mathcal{P}$ be the prime divisors of n, where $r \in \mathbb{N}_0$. Then $|g| = n$ if and only if $g^{\frac{n}{p_i}} \neq 1$ for all $i \in \{1, \ldots, r\}$.

Proof. a) For $i \in \mathbb{Z}$ we have $i \in I(g^k)$, that is $g^{ik} = 1$, if and only if $n \mid ik$, which holds if and only if $\frac{n}{\gcd_+(k,n)} \mid i$; entailing $I(g^k) = \frac{n}{\gcd_+(k,n)} \cdot \mathbb{Z} \trianglelefteq \mathbb{Z}$.

b) If $|g| = n$ then g has the required properties. Conversely, let g fulfill these conditions. Then from $g^n = 1$ we infer that $|g| \mid n$. Assume that $|g| < n$, then $|g|$ is a proper divisor of n, and thus using the factorisation of n we infer that $|g| \mid \frac{n}{p_i}$, for some $i \in \{1, \ldots, r\}$, entailing $g^{\frac{n}{p_i}} = 1$, a contradiction. ♯

(10.4) Cyclic groups. Let G be a group. Then G is called **cyclic**, if there is $g \in G$ such that $G = \langle g\rangle$. In this case we write $G \cong C_{|g|}$. For example, we have $(\mathbb{Z}, +) = \langle 1\rangle = \langle -1\rangle$, which is infinite, and for $n \in \mathbb{N}$ we have $(\mathbb{Z}/n\mathbb{Z}, +) = \langle 1\rangle$, hence the latter is cyclic of order n.

Theorem: Characterisation of cyclic groups. Let G be finite.

a) Let G be cyclic. Then any subgroup of G is cyclic as well. There is a subgroup of G of order $d \in \mathbb{N}$ if and only if $d \mid |G|$; in this case it is uniquely determined.

In particular, there are precisely $\varphi(|G|)$ elements of G which can be chosen as a generator, where φ denotes Euler's totient function.

b) The group G is cyclic if and only if G has at most one subgroup of order d for any $d \in \mathbb{N}$. In particular, if $|G|$ is a prime then G is cyclic.

Proof. a) Let $G = \langle g\rangle$ such that $n := |G|$. For $U \leq G$ let $I_U(g) := \{i \in \mathbb{Z}; g^i \in U\}$. Then we have $g^0 = 1 \in U$, and for $i, j \in I_U(g)$ we have $g^{-i} = (g^i)^{-1} \in U$ and $g^{i+j} = g^i g^j \in U$, showing that $I_U(g) \subseteq \mathbb{Z}$ is an additive subgroup; and for $k \in \mathbb{Z}$ we get $g^{ik} = (g^i)^k \in U$, showing that $I_U(g) \trianglelefteq \mathbb{Z}$ is an ideal. Hence we have $I_U(g) = m\mathbb{Z}$, for some $m \in \mathbb{N}$, and thus $U = \langle g^m\rangle$.

Since the order of any subgroup of G divides $|G|$, we only have to show existence and uniqueness in this case: Hence let $d \mid n$ and $m := \frac{n}{d} \in \mathbb{N}$. Then $U := \langle g^m\rangle \leq G$ has order $|g^m| = \frac{n}{m} = d$. As for uniqueness, if $k \in \mathbb{Z}$ such that $|g^k| = d$, then we have $\frac{n}{\gcd_+(k,n)} = d = \frac{n}{m}$, hence $m = \gcd_+(k,n) \mid k$. This implies $g^k \in \langle g^m\rangle = U$, thus U contains all elements of G of order d.

This proves a). Before proceeding we note that, counting the possible generators of all subgroups of G, we have shown that $\sum_{d\in\mathbb{N},d\,|\,n}\varphi(d)=n$.

b) If G is cyclic, then we have just seen that G has the required property. To show the converse, let G fulfill the assumption on the subgroup structure, where $n:=|G|$. Given $d\in\mathbb{N}$, there is an element of G of order d only if $d\mid n$. In this case, if there is an element $g\in G$ of order d, then $\langle g\rangle\leq G$ is the unique subgroup of order d. Thus all elements of order d generate one and the same subgroup, which is cyclic, and thus has precisely $\varphi(d)$ elements of order d. Hence the number of all elements of order $d<n$ is bounded above by $\sum_{d\,|\,n,d\neq n}\varphi(d)=n-\varphi(n)<n$. Thus there is an element of order n. ♯

(10.5) Prime residue classes. The preceeding considerations imply the following classical theorems due to Euler, Fermat and Wilson, but we also provide direct proofs:

Euler's Theorem [1735]. For $n\in\mathbb{N}$ and $\overline{a}\in(\mathbb{Z}/n\mathbb{Z})^*$ we have $\overline{a}^{\varphi(n)}=\overline{1}$.

Proof. This follows from $|\overline{a}|\mid|(\mathbb{Z}/n\mathbb{Z})^*|=\varphi(n)$.

More directly, we may proceed as follows: For $\overline{a}\in(\mathbb{Z}/n\mathbb{Z})^*$ we consider the bijection $\lambda_{\overline{a}}\colon\mathbb{Z}/n\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}\colon\overline{x}\mapsto\overline{ax}$. Since for $\overline{x}\in(\mathbb{Z}/n\mathbb{Z})^*$ we have $\overline{ax}\in(\mathbb{Z}/n\mathbb{Z})^*$ as well, we infer that $\lambda_{\overline{a}}$ restricts to a bijection $\lambda_{\overline{a}}\colon(\mathbb{Z}/n\mathbb{Z})^*\to(\mathbb{Z}/n\mathbb{Z})^*$. Hence we have $\overline{a}^{\varphi(n)}\cdot\prod_{\overline{x}\in(\mathbb{Z}/n\mathbb{Z})^*}\overline{x}=\prod_{\overline{x}\in(\mathbb{Z}/n\mathbb{Z})^*}\overline{ax}=\prod_{\overline{x}\in(\mathbb{Z}/n\mathbb{Z})^*}\overline{x}\in(\mathbb{Z}/n\mathbb{Z})^*$, thus multiplying with $\big(\prod_{\overline{x}\in(\mathbb{Z}/n\mathbb{Z})^*}\overline{x}\big)^{-1}\in(\mathbb{Z}/n\mathbb{Z})^*$ yields $\overline{a}^{\varphi(n)}=\overline{1}\in(\mathbb{Z}/n\mathbb{Z})^*$. ♯

Fermat's Theorem [1640]. For $p\in\mathcal{P}$ and $\overline{a}\in(\mathbb{Z}/p\mathbb{Z})^*=(\mathbb{Z}/p\mathbb{Z})\setminus\{\overline{0}\}$ we have $\overline{a}^{p-1}=\overline{1}\in(\mathbb{Z}/p\mathbb{Z})^*$; thus for all $\overline{a}\in\mathbb{Z}/p\mathbb{Z}$ we have $\overline{a}^p=\overline{a}\in\mathbb{Z}/p\mathbb{Z}$.

Proof. For $\overline{a}\neq\overline{0}$ this is Euler's Theorem for the special case of prime moduli.

Again, more directly we may proceed as follows: First note that for $i\in\{0,\dots,p\}$ we have $\binom{p}{i}=\frac{p\cdot(p-1)\cdots(p-i+1)}{i\cdot(i-1)\cdots1}\in\mathbb{Z}$, thus for $i\notin\{0,p\}$ we have $\binom{p}{i}\equiv0\pmod p$, while $\binom{p}{0}=\binom{p}{p}=1$. Now we show that $a^p\equiv a\pmod p$, for $a\in\mathbb{N}_0$, proceeding by induction: The case $a=0$ being trivial, let $a\geq1$. Then we have $(a+1)^p\equiv\sum_{i=0}^p\binom{p}{i}a^i\equiv a^p+1\equiv a+1\pmod p$.

In other words, we have $\overline{a}^p=\overline{a}\in\mathbb{Z}/p\mathbb{Z}$, for $\overline{a}\in\mathbb{Z}/p\mathbb{Z}$. If $\overline{a}\neq\overline{0}$, then $\overline{a}\in(\mathbb{Z}/p\mathbb{Z})^*$, thus multiplying with $\overline{a}^{-1}\in(\mathbb{Z}/p\mathbb{Z})^*$ yields $\overline{a}^{p-1}=\overline{1}\in(\mathbb{Z}/p\mathbb{Z})^*$. ♯

Wilson's Theorem [1770]. Let $1\neq n\in\mathbb{N}$. Then n is a prime if and only if $(n-1)!\equiv-1\pmod n$. In this case, if n is an odd prime, then we have $\big((\frac{n-1}{2})!\big)^2\equiv(-1)^{\frac{n+1}{2}}\pmod n$.

Proof. Let n be decomposable. We prove slightly more than asserted: If $n = 4$ then $3! \equiv 2 \pmod 4$; if $n = p^2$ for an odd prime p, then $n > 2p$ implies $n = p^2 \mid (n-1)!$, thus $(n-1)! \equiv 0 \pmod n$. Thus we may assume that $n = ab$ where $1 < a < b < n$, hence $n = ab \mid (n-1)!$, thus $(n-1)! \equiv 0 \pmod n$.

Let now $n = p$ be a prime. Then, by Fermat's Theorem, for all $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^*$ we have $\overline{a}^{p-1} = \overline{1}$, hence $(\mathbb{Z}/p\mathbb{Z})^*$ is the set of roots of $X^{p-1} - \overline{1} \in \mathbb{Z}/p\mathbb{Z}[X]$, thus $X^{p-1} - \overline{1} = \prod_{\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^*} (X - \overline{a}) \in \mathbb{Z}/p\mathbb{Z}[X]$. Evaluating at $X \mapsto 0$ yields $\prod_{\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^*} \overline{a} = (-\overline{1})^{p-2} \in \mathbb{Z}/p\mathbb{Z}$, entailing the first assertion.

Alternatively, without invoking Fermat's Theorem, we may argue as follows: We may assume that p is odd. Then for $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^*$ we have $\overline{a} = \overline{a}^{-1}$ if and only if $\overline{a}^2 = \overline{1}$, that is $\overline{a}$ is a root of $X^2 - \overline{1} = (X - \overline{1})(X + \overline{1}) \in \mathbb{Z}/p\mathbb{Z}[X]$, which thus holds if and only if $\overline{a} \in \{\pm\overline{1}\}$. Hence pairing elements with their inverses yields $\prod_{\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^* \setminus \{\pm\overline{1}\}} \overline{a} = \overline{1}$, thus $-\overline{1} \cdot \overline{1} \cdot \prod_{\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^* \setminus \{\pm\overline{1}\}} \overline{a} = -\overline{1} \in (\mathbb{Z}/p\mathbb{Z})^*$.

Finally, for an odd prime p we have $-1 \equiv (p-1)! \equiv (\frac{p-1}{2})! \cdot \prod_{i=1}^{\frac{p-1}{2}} (p-i) \equiv (-1)^{\frac{p-1}{2}} \cdot \big((\frac{p-1}{2})!\big)^2 \pmod p$, implying the second assertion. ♯

(10.6) Prime moduli. The basic structural observation is the following theorem, which in its general form is due to Artin, but the number theoretic case was already known to Gauss.

Artin's Theorem. Let K be a field and $G \leq K^*$ be finite. Then G is cyclic.

Proof. Let $U \leq G$ be a subgroup of order $d \in \mathbb{N}$. Then all elements of U have order dividing d, and thus are roots of the polynomial $X^d - 1 \in K[X]$. Since K is a field, there are at most d such roots in K. Hence U consists of all elements of G of order dividing d, thus U is uniquely determined. This shows that G has at most one subgroup of order d for any $d \in \mathbb{N}$, thus G is cyclic. ♯

In particular, if $d \in \mathbb{Z}$ such that $d < 0$ and squarefree, then $\mathbb{Z}[\sqrt{d}] \subseteq \mathbb{Q}[\sqrt{d}]$, and $\mathbb{Z}[\frac{1+\sqrt{d}}{2}] \subseteq \mathbb{Q}[\sqrt{d}]$ whenever $4 \mid (d-1)$, have finite groups of units, hence these are cyclic: Indeed, for $d \neq -1$ we have $\mathbb{Z}[\sqrt{d}]^* = \{\pm 1\} \cong C_2$, while $\mathbb{Z}[i]^* = \{1, i, i^2, i^3\} \cong C_4$; for $4 \mid (d-1)$ and $d \neq -3$ we have $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]^* = \{\pm 1\} \cong C_2$, while $\mathbb{Z}[\zeta_6^* = \{1, \zeta_6, \zeta_6^2, \ldots, \zeta_6^5\} \cong C_6$, where $\zeta_6 := \frac{1+\sqrt{-3}}{2}$.

More interestingly, if $p \in \mathcal{P}$ then $(\mathbb{Z}/p\mathbb{Z})^* \cong C_{p-1}$ is cyclic [Gauss, 1798]. An element $\overline{\rho} \in (\mathbb{Z}/p\mathbb{Z})^*$ such that $\langle\overline{\rho}\rangle = (\mathbb{Z}/p\mathbb{Z})^*$, that is having order $p-1$, is called a **primitive root** modulo p. There are precisely $\varphi(p-1)$ primitive roots modulo p, which for a fixed one ρ are given as $\{\overline{\rho}^k \in (\mathbb{Z}/p\mathbb{Z})^*; \overline{k} \in (\mathbb{Z}/(p-1)\mathbb{Z})^*\}$. Hence it suffices to determine the smallest positive primitive root $\rho \in \mathbb{Z}_p$; those for $p < 1000$ have been found by Jacobi [1839], and are given in Table 8.

Artin's Conjecture [1927] says that any $a \in \mathbb{Z} \setminus \big(\{-1\} \cup \{b^2 \in \mathbb{Z}; b \in \mathbb{Z}\}\big)$ is a primitive root modulo infinitely many primes. Note that indeed $\overline{0} \notin (\mathbb{Z}/p\mathbb{Z})^*$ and $-\overline{1} \in (\mathbb{Z}/p\mathbb{Z})^*$ has order 2, for any odd prime p, and that $a = b^2$, for some

Table 8: Smallest primitive roots.

ρ	$p < 1000$
1	2
2	3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83, 101, 107, 131, 139, 149, 163, 173, 179, 181, 197, 211, 227, 269, 293, 317, 347, 349, 373, 379, 389, 419, 421, 443, 461, 467, 491, 509, 523, 541, 547, 557, 563, 587, 613, 619, 653, 659, 661, 677, 701, 709, 757, 773, 787, 797, 821, 827, 829, 853, 859, 877, 883, 907, 941, 947
3	7, 17, 31, 43, 79, 89, 113, 127, 137, 199, 223, 233, 257, 281, 283, 331, 353, 401, 449, 463, 487, 521, 569, 571, 593, 607, 617, 631, 641, 691, 739, 751, 809, 811, 823, 857, 881, 929, 953, 977
5	23, 47, 73, 97, 103, 157, 167, 193, 263, 277, 307, 383, 397, 433, 503, 577, 647, 673, 683, 727, 743, 863, 887, 937, 967, 983
6	41, 109, 151, 229, 251, 271, 367, 733, 761, 971, 991
7	71, 239, 241, 359, 431, 499, 599, 601, 919, 997
10	313, 337
11	643, 719, 769, 839
13	457, 479
15	439
17	311, 911
19	191
21	409

$0 \neq b \in \mathbb{Z}$, implies $\overline{a}^{\frac{p-1}{2}} = \overline{b}^{p-1} = \overline{1} \in (\mathbb{Z}/p\mathbb{Z})^*$ for any odd prime p such that $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^*$, which in particular encompasses all odd primes $p > a$.

Corollary. For $p \in \mathcal{P}$ odd, the congruence $X^2 \equiv -1 \pmod{p}$ is solvable if and only if $p \equiv 1 \pmod{4}$; in this case, the solutions are $\pm\overline{(\frac{p-1}{2})!} \in \mathbb{Z}/p\mathbb{Z}$.

Proof. The solutions of the congruence in question are precisely the elements $\overline{x} \in (\mathbb{Z}/p\mathbb{Z})^*$ fulfilling $\overline{x}^2 = -\overline{1}$. Since this implies $\overline{x}^4 = \overline{1}$, these are precisely the elements of $(\mathbb{Z}/p\mathbb{Z})^*$ of order 4. Now we have $(\mathbb{Z}/p\mathbb{Z})^* \cong C_{p-1}$, hence $(\mathbb{Z}/p\mathbb{Z})^*$ has elements of order 4 if and only if $p \equiv 1 \pmod{4}$.

In this case, there are $\varphi(4) = 2$ such elements. (This is consistent with the fact that the polynomial $X^2 + \overline{1} \in \mathbb{Z}/p\mathbb{Z}[X]$ has at most two roots in $\mathbb{Z}/p\mathbb{Z}$.) Finally, it follows from Wilson's Theorem that $\left((\frac{p-1}{2})!\right)^2 \equiv -1 \pmod{p}$, ♯

11 Groups of prime residues

(11.1) The group of prime residue classes. Given $n = \prod_{i=1}^{r} p_i^{a_i} \in \mathbb{N}$, where $p_i \in \mathcal{P}$ are pairwise distinct, $a_i \in \mathbb{N}$ and $r \in \mathbb{N}_0$, the Chinese remainder theorem

implies $\mathbb{Z}/n\mathbb{Z} \cong \bigoplus_{i=1}^{r} \mathbb{Z}/p_i^{a_i}\mathbb{Z}$ as commutative rings, hence for the associated groups of units we have, as commutative groups:

$$(\mathbb{Z}/n\mathbb{Z})^* \cong \prod_{i=1}^{r} (\mathbb{Z}/p_i^{a_i}\mathbb{Z})^*.$$

Thus, in order to describe the group structure of $(\mathbb{Z}/n\mathbb{Z})^*$, it suffices to deal with the groups $(\mathbb{Z}/p^k\mathbb{Z})^*$, where $p \in \mathcal{P}$ and $k \in \mathbb{N}$.

(11.2) Prime power moduli. The structure of $(\mathbb{Z}/p^k\mathbb{Z})^*$, where $p \in \mathcal{P}$ and $k \in \mathbb{N}$, is elucidated by the theorem to follow; recall that $|(\mathbb{Z}/p^k\mathbb{Z})^*| = \varphi(p^k) = (p-1)p^{k-1}$. To proceed, we need a purely group theoretic lemma first:

Lemma. Let G be a commutative finite group, and let $g, h \in G$.

a) If $\langle g\rangle \cap \langle h\rangle = \{1\}$ then we have $\langle g, h\rangle \cong \langle g\rangle \times \langle h\rangle$, in particular $|\langle g, h\rangle| = |g|\cdot|h|$.

b) If $\gcd_+(|g|, |h|) = 1$ then $\langle g\rangle \cap \langle h\rangle = \{1\}$, and $\langle g, h\rangle = \langle gh\rangle$ is cyclic.

Proof. a) Let $n := |g| \in \mathbb{N}$ and $m := |h| \in \mathbb{N}$. Then we have $\langle g, h\rangle = \{g^i h^j \in G; i \in \mathbb{Z}_n, j \in \mathbb{Z}_m\} \leq G$: Since G is commutative, the right hand side indeed is a subgroup, which is necessarily contained in any subgroup containing $\{g, h\}$. Letting $i, i' \in \mathbb{Z}_n$ and $j, j' \in \mathbb{Z}_m$ such that $g^i h^j = g^{i'} h^{j'}$, we get $g^{i-i'} = h^{j'-j} \in \langle g\rangle \cap \langle h\rangle = \{1\}$, thus $g^i = g^{i'}$ and $h^j = h^{j'}$, entailing $i = i'$ and $j = j'$. Hence we have $|\langle g, h\rangle| = nm$, and thus any element of $\langle g, h\rangle$ can be written uniquely as $g^i h^j$, where $i \in \mathbb{Z}_n$ and $j \in \mathbb{Z}_m$. In other words, we have $\langle g, h\rangle \cong \langle g\rangle \times \langle h\rangle$.

b) For $x \in \langle g\rangle \cap \langle h\rangle$ we have $|x| \mid \gcd_+(n, m) = 1$, implying $\langle g\rangle \cap \langle h\rangle = \{1\}$, hence $\langle g, h\rangle \cong \langle g\rangle \times \langle h\rangle$. Thus, by uniqueness, for $k \in \mathbb{Z}$ we have $(gh)^k = g^k h^k = 1$ if and only if $nm = \mathrm{lcm}_+(n, m) \mid k$, hence $|gh| = nm = |\langle g, h\rangle|$. ♯

Theorem. a) Let $p \in \mathcal{P}$ be odd, and let $\rho \in \mathbb{Z}$ be a primitive root modulo p. Then for $k \in \mathbb{N}$ we have $(\mathbb{Z}/p^k\mathbb{Z})^* \cong \langle \overline{\rho}_k\rangle \times \langle \overline{1+p}\rangle \cong C_{p-1} \times C_{p^{k-1}} \cong C_{(p-1)p^{k-1}}$, where $\overline{\rho}_k := \overline{\rho}^{p^{k-1}}$ has order $p-1$, and $\overline{1+p}$ has order p^{k-1}.

b) For $k \geq 2$ we have $(\mathbb{Z}/2^k\mathbb{Z})^* \cong \langle -\overline{1}\rangle \times \langle \overline{5}\rangle \cong C_2 \times C_{2^{k-2}}$, where $\overline{5} = \overline{1+2^2}$ has order 2^{k-2}; hence $(\mathbb{Z}/2^k\mathbb{Z})^*$ is not cyclic for $k \geq 3$, while $(\mathbb{Z}/4\mathbb{Z})^* = \{-\overline{1}\} \cong C_2$ and $(\mathbb{Z}/2\mathbb{Z})^* = \{\overline{1}\}$.

Proof. i) For p odd, we first specify an element $\overline{\rho}_k \in (\mathbb{Z}/p^k\mathbb{Z})^*$ of order $p-1$:

We consider the polynomial $g := X^{p-1} - 1 \in \mathbb{Z}[X]$, whose Hasse-Teichmüller derivatives are given as $g^{[j]} = \binom{p-1}{j} X^{p-1-j} \in \mathbb{Z}[X]$, for $j \in \{1, \ldots, p-1\}$. Since $\binom{p-1}{j} \not\equiv 0 \pmod{p}$, for any $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^*$ we get $g^{[j]}(a) \not\equiv 0 \pmod{p}$. Now let $\overline{\rho}_1 := \overline{\rho} \in (\mathbb{Z}/p\mathbb{Z})^*$ be a primitive root. Hence proceeding by induction on $k \in \mathbb{N}$, (linear) Hensel lifting shows that there there is a unique element $\overline{\rho}_{k+1} \in (\mathbb{Z}/p^{k+1}\mathbb{Z})^*$ such that $\rho_{k+1} - \rho_k \equiv 0 \pmod{p^k}$ and $\rho_{k+1}^{p-1} \equiv 1 \pmod{p^{k+1}}$.

Now $\overline{\rho}_{k+1}$ is found as follows: We have $g^{[1]}(\rho_k) \equiv (p-1)\rho_k^{p-2} \equiv -\rho_k^{-1} \pmod{p}$. Hence letting $g(\rho_k) = \rho_k^{p-1} - 1 = b_k p^k$, for some $b_k \in \mathbb{Z}$, and $y \in \mathbb{Z}$ such that $y \equiv -b_k \cdot (-\rho_k^{-1})^{-1} \equiv b_k \rho_k \pmod{p}$, we get $\rho_{k+1} \equiv \rho_k + \rho_k b_k p^k \equiv \rho_k(1 + b_k p^k) \equiv \rho_k^p \pmod{p^{k+1}}$. Hence by induction on $k \in \mathbb{N}$ we get $\rho_{k+1} = \rho^{p^{k-1}} \pmod{p^{k+1}}$.

By construction we have $\overline{\rho}_k^{p-1} = \overline{1} \in (\mathbb{Z}/p^k\mathbb{Z})^*$, hence $\overline{\rho}_k$ has order dividing $p-1$. But since $\rho_k \equiv \rho \pmod{p}$, and $\overline{\rho} \in (\mathbb{Z}/p\mathbb{Z})^*$ has order $p-1$, using the natural map $\nu_p^{p^k} : \mathbb{Z}/p^k\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ we conclude that $\overline{\rho}_k$ has order $p-1$ as well.

ii) For p arbitrary, we specifiy elements of $(\mathbb{Z}/p^k\mathbb{Z})^*$ of maximum p-power order:

For any $p \in \mathcal{P}$ and $k \in \mathbb{N}_0$ and $j \in \{1, \ldots, p^k\}$ we have $\binom{p^k}{j} = \frac{1}{j!} \cdot \prod_{i=0}^{j-1}(p^k - i) \in \mathbb{Z}$, and thus $\nu_p\big(\binom{p^k}{j}\big) = k + \nu_p((j-1)!) - \nu_p(j!) = k - \nu_p(j)$. Moreover, we have $j > \nu_p(j)$ for all $j \in \mathbb{N}$, where for p odd we have $j \geq \nu_p(j) + 2$ for all $j \geq 2$, while for $p = 2$ we have $j \geq \nu_2(j) + 2$ for all $j \geq 3$.

We consider the polynomial $f_k := X^{p^k} - 1 \in \mathbb{Z}[X]$, whose Hasse-Teichmüller derivatives are given as $f_k^{[j]} = \binom{p^k}{j} X^{p^k - j} \in \mathbb{Z}[X]$, for $j \in \{1, \ldots, p^k\}$. Evaluating at 1 yields $f_k^{[j]}(1) = \binom{p^k}{j} \in \mathbb{Z}$. Hence applying Taylor expansion, using $f_k(1) = 0$, for all $a \in \mathbb{Z}$ we obtain $(1+a)^{p^k} - 1 = f_k(1+a) = \sum_{j=0}^{p^k} f_k^{[j]}(1) \cdot a^j = \sum_{j=1}^{p^k} \binom{p^k}{j} \cdot a^j = p^k \cdot a + \sum_{j=2}^{p^k} \binom{p^k}{j} \cdot a^j \in \mathbb{Z}$. Now we distinguish two cases:

ii) a) Let p be odd and $k \geq 2$, and let $a := p$. Then we get $(1+p)^{p^{k-2}} - 1 = f_{k-2}(1+p) = p^{k-1} + \sum_{j=2}^{p^{k-2}} \binom{p^{k-2}}{j} \cdot p^j$. We have $\nu_p\big(\binom{p^{k-2}}{j} \cdot p^j\big) = (k-2) - \nu_p(j) + j \geq k$, for $j \geq 2$. Hence we infer that $(1+p)^{p^{k-2}} \equiv 1 + p^{k-1} \pmod{p^k}$. Next we get $(1+p^{k-1})^p - 1 = f_1(1+p^{k-1}) = \sum_{j=1}^{p} \binom{p}{j} \cdot p^{j(k-1)}$. We have $\nu_p\big(\binom{p}{j} \cdot p^{j(k-1)}\big) = 1 + j(k-1) \geq 1 + (k-1) = k$ for $j < p$, while for $j = p$ we get $\nu_p\big(\binom{p}{p} \cdot p^{p(k-1)}\big) = p(k-1) \geq k$; note that the latter inequality is equivalent to $k \geq \frac{p}{p-1}$. Thus we have $(1+p^{k-1})^p \equiv 1 \pmod{p^k}$. Hence we get $(1+p)^{p^{k-1}} \equiv ((1+p)^{p^{k-2}})^p \equiv (1+p^{k-1})^p \equiv 1 \pmod{p^k}$, from which we conclude that $\overline{1+p} \in (\mathbb{Z}/p^k\mathbb{Z})^*$ has order p^{k-1}.

ii) b) Let $p := 2$ and $k \geq 3$, and let $a := 4$. Then we get $(1+4)^{2^{k-3}} - 1 = f_{k-3}(1+4) = 2^{k-1} + \sum_{j=2}^{2^{k-3}} \binom{2^{k-3}}{j} \cdot 4^j$. We have $\nu_p\big(\binom{2^{k-3}}{j} \cdot 4^j\big) = (k-3) - \nu_2(j) + 2j \geq k$ for $j \geq 3$, while for $j = 2$ we get $\nu_p\big(\binom{2^{k-3}}{2} \cdot 4^2\big) = (k-3) - \nu_2(2) + 4 \geq k$. Hence we infer that $(1+4)^{2^{k-3}} \equiv 1 + 2^{k-1} \pmod{2^k}$.

Next we get $(1+2^{k-1})^2 - 1 = f_1(1+2^{k-1}) = 2^k + 2^{2k-2}$. Thus we have $(1+2^{k-1})^2 \equiv 1 \pmod{2^k}$. Hence we get $(1+4)^{2^{k-2}} \equiv ((1+4)^{2^{k-3}})^2 \equiv (1 + 2^{k-1})^2 \equiv 1 \pmod{2^k}$, which shows that $\overline{1+4} \in (\mathbb{Z}/2^k\mathbb{Z})^*$ has order 2^{k-2}.

iii) Let p be odd, and let $\sigma := \overline{\rho}_k$ and $\tau := \overline{1+p}$. Then $\gcd_+(|\overline{\rho}_k|, |\overline{1+p}|) = \gcd_+(p-1, p^{k-1}) = 1$ and $|\overline{\rho}_k| \cdot |\overline{1+p}| = (p-1)p^{k-1} = |(\mathbb{Z}/p^k\mathbb{Z})^*|$ shows that $(\mathbb{Z}/p^k\mathbb{Z})^* \cong \langle \overline{\rho}_k \rangle \times \langle \overline{1+p} \rangle$.

Table 9: Powers of a primitive root modulo 5.

k	1	2	3	4	5	6	7	8	9	10
ρ_k	2	7	57	182	2057	14557	45807	280182	280182	6139557
					-1068	-1068	-32318	-110443		-3626068

Let finally $p := 2$, let $k \geq 3$, and let $\sigma := -\overline{1}$ and $\tau := \overline{1+2^2}$. Then $\tau^{2^{k-3}} = \overline{1+2^{k-1}} \in \langle\tau\rangle$ is the unique element of $\langle\tau\rangle$ of order 2. Hence from $\overline{1+2^{k-1}} \neq \sigma$ we conclude that $\langle\sigma\rangle \cap \langle\tau\rangle = \{\overline{1}\}$. Since $|\sigma| \cdot |\tau| = 2 \cdot 2^{k-2} = 2^{k-1} = |(\mathbb{Z}/2^k\mathbb{Z})^*|$ we infer that $(\mathbb{Z}/2^k\mathbb{Z})^* \cong \langle\sigma\rangle \times \langle\tau\rangle$. Moreover, since $(\mathbb{Z}/2^k\mathbb{Z})^*$ has at least two elements of order 2, this group is not cyclic. ♯

Example. For $p := 3$ and $\rho := -1$ we get $\rho_k = -1$, for $k \in \mathbb{N}$. For $p := 5$ and $\rho := 2$ a few powers are shown in Table 9, where we also give the numerically smallest residue in $\mathbb{Z}/5^k\mathbb{Z}$ if it is negative.

(11.3) Corollary: Gauss. Let $n \in \mathbb{N}$. Then $(\mathbb{Z}/n\mathbb{Z})^*$ is cyclic if and only if $n \in \{1, 2, 4\} \cup \{p^k, 2p^k; p \in \mathcal{P} \text{ odd}, k \in \mathbb{N}\}$

Proof. Let $n = 2^a \cdot \prod_{i=1}^r p_i^{a_i} \in \mathbb{N}$, where $2 \neq p_i \in \mathcal{P}$ are pairwise distinct, $a \in \mathbb{N}_0$ and $a_i \in \mathbb{N}$, for some $r \in \mathbb{N}_0$. Then we have $(\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/2^a\mathbb{Z})^* \times \prod_{i=1}^r (\mathbb{Z}/p_i^{a_i}\mathbb{Z})^*$. Since each group $(\mathbb{Z}/p_i^{a_i}\mathbb{Z})^* \cong C_{p_i-1} \times C_{p_i^{a_i-1}}$ has an element of order 2, we conclude that $(\mathbb{Z}/n\mathbb{Z})^*$ is not cyclic whenever $r \geq 2$.

If $a \geq 3$ then $(\mathbb{Z}/2^a\mathbb{Z})^* \cong C_2 \times C_{2^{a-2}}$ is not cyclic, hence $(\mathbb{Z}/n\mathbb{Z})^*$ neither is. If $r = 0$, then $(\mathbb{Z}/2^a\mathbb{Z})^*$ is cyclic if and only if $a \leq 2$.

Let $r = 1$. If $a = 2$, then both $(\mathbb{Z}/p_1^{a_1}\mathbb{Z})^*$ and $(\mathbb{Z}/2^a\mathbb{Z})^*$ have an element of order 2, thus $(\mathbb{Z}/n\mathbb{Z})^*$ is not cyclic; if $a \leq 1$, then $(\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/p_1^{a_1}\mathbb{Z})^*$ is cyclic. ♯

12 Quadratic residues

(12.1) Quadratic congruences. We consider the question when the quadratic congruence $X^2 \equiv a \pmod{n}$, where $n \in \mathbb{N}$ and $a \in \mathbb{Z}$, is solvable. Being a special case of a polynomial congruence (actually the easiest one next to the linear case), by the Chinese remainder theorem this question is reduced to congruences $X^2 \equiv a \pmod{p^k}$, where $p \in \mathcal{P}$ and $k \in \mathbb{N}$. The latter can be treated by a further reduction to the case of congruences $X^2 \equiv a \pmod{p}$, and subsequent lifting. In order to proceed along these lines, we need a purely group theoretic lemma first:

Lemma. Let $G = \langle\gamma\rangle \cong C_n$ be a cyclic group of even order $n \in \mathbb{N}$.

a) We have a surjective group homomorphism $q\colon G \to \{\pm 1\}\colon \gamma^i \mapsto (-1)^i$;

b) Let $\mathcal{Q} := \{g^2 \in G; g \in G\}$ be the set of **squares** in G. Then we have $\mathcal{Q} = \langle\gamma^2\rangle = \{g \in G; q(g) = 1\} \leq G$, the unique subgroup of order $\frac{n}{2}$.

c) Let $z := \gamma^{\frac{n}{2}} \in G$ be the unique element of order 2. Then for any $g \in G$ we have $g^{\frac{n}{2}} \in \langle z\rangle$, where $g \in \mathcal{Q}$ if and only if $g^{\frac{n}{2}} = 1$.

Proof. a) Transporting the natural ring homomorphism $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ with the group isomorphisms $(\mathbb{Z}/n\mathbb{Z}, +) \to G\colon \bar{i} \mapsto \gamma^i$ and $(\mathbb{Z}/2\mathbb{Z}, +) \to \{\pm 1\}\colon \bar{j} \mapsto (-1)^j$ yields the group homomorphism $q\colon G \to \{\pm 1\}\colon \gamma^i \mapsto (-1)^i$.

b) If $g \in \langle\gamma^2\rangle$, then $g = (\gamma^2)^i = (\gamma^i)^2$ for some $i \in \mathbb{Z}$, hence $g \in \mathcal{Q}$. Conversely, if $g = h^2 \in G$, then there is $i \in \mathbb{Z}$ such that $h = \gamma^i$, hence $g = (\gamma^i)^2 = (\gamma^2)^i \in \langle\gamma^2\rangle$. Thus $\mathcal{Q} = \langle\gamma^2\rangle$, where $|\gamma^2| = \frac{|\gamma|}{\gcd_+(2,|\gamma|)} = \frac{n}{2}$; with uniqueness since G is cyclic.

Moreover, if $g \in \mathcal{Q}$ then q being a homomorphism implies that $q(g) = 1$. Conversely, if $g = \gamma^i \in G$, for some $i \in \mathbb{Z}$, from $1 = q(g) = q(\gamma^i) = (-1)^i$ we infer that i is even, hence $g \in \langle\gamma^2\rangle = \mathcal{Q}$.

c) We have $z \neq 1$ and $z^2 = (\gamma^{\frac{n}{2}})^2 = \gamma^n = 1 \in G$, hence z has order 2; with uniqueness since G is cyclic. Now let $g \in G$. Then $(g^{\frac{n}{2}})^2 = g^n = 1$ shows that g has order dividing 2, hence $g \in \langle z\rangle$. Moreover, we have $g^{\frac{n}{2}} = 1$ if and only if g has order dividing $\frac{n}{2}$, which holds if and only if g is contained in the unique subgroup of order $\frac{n}{2}$, which equals $\mathcal{Q}$. ♯

Let $\mathcal{N} := G \setminus \mathcal{Q}$ be the set of **non-squares** in G. Thus we have $\mathcal{Q} = \{\gamma^{2i} \in G; i \in \mathbb{Z}_{\frac{n}{2}}\}$ and $\mathcal{N} = \{\gamma^{2i+1} \in G; i \in \mathbb{Z}_{\frac{n}{2}}\} = \mathcal{Q}\gamma$, hence $G = \mathcal{Q} \dot\cup \mathcal{N} = \mathcal{Q} \dot\cup \mathcal{Q}\gamma$ is the partition of G into $\mathcal{Q}$-cosets; in particular we have $|\mathcal{Q}| = |\mathcal{N}| = \frac{n}{2}$.

(12.2) Quadratic congruences modulo prime powers. We consider the quadratic congruence $X^2 \equiv a \pmod{p^k}$, where $p \in \mathcal{P}$ and $k \in \mathbb{N}$ and $a \in \mathbb{Z}$. The particular case of $a \not\equiv 0 \pmod{p}$ admits a systematic treatment:

Theorem. Let $p \in \mathcal{P}$ and $k \in \mathbb{N}$, and let $a \in \mathbb{Z}$ such that $p \nmid a$.

a) Let p be odd. Then the congruence $X^2 \equiv a \pmod{p^k}$ has a solution if and only if the congruence $X^2 \equiv a \pmod{p}$ has. In this case, there are precisely two solutions modulo p^k, which just differ by sign.

b) Let $p = 2$, and let $l := \min\{3, k\}$. Then the congruence $X^2 \equiv a \pmod{2^k}$ has a solution if and only if $a \equiv 1 \pmod{2^l}$. In this case, for $k \geq 3$ there are precisely 4 solutions modulo 2^k, while for $k = 2$ there are precisely 2 solutions modulo 4, and for $k = 1$ there is a unique solution modulo 2.

Proof. a) If $X^2 \equiv a \pmod{p^k}$ has a solution then $X^2 \equiv a \pmod{p}$ also has. We consider the converse: Let $x_1 \in \mathbb{Z}$ such that $x_1^2 \equiv a \pmod{p}$; hence there

are precisely two solutions $\pm\overline{x}_1 \in (\mathbb{Z}/p\mathbb{Z})^*$. Let $f := X^2 - a \in \mathbb{Z}[X]$, hence we have $f^{(1)} = 2X \in \mathbb{Z}[X]$. Since $f^{(1)}(\pm x_1) \not\equiv 0 \pmod{p}$, by Hensel lifting for any $k \in \mathbb{N}$ there are unique $\pm\overline{x}_k \in (\mathbb{Z}/p^k\mathbb{Z})^*$ such that $\pm x_k \equiv \pm x_1 \pmod{p}$ and $(\pm x_k)^2 \equiv a \pmod{p^k}$. (Note that this argument breaks down for $p = 2$, so that we have to argue differently in this case.)

b) If $X^2 \equiv a \pmod{2^k}$ has a solution then $X^2 \equiv a \pmod{2^l}$ also has; and if $\overline{x}_l \in (\mathbb{Z}/2^l\mathbb{Z})^*$ is a solution, then we get $\overline{a} = \overline{x}_l^2 = \overline{1} \in (\mathbb{Z}/2^l\mathbb{Z})^*$. We consider the converse: For $k \leq 3$, hence $l = k$, we have $(\mathbb{Z}/2\mathbb{Z})^* = \{\overline{1}\}$ and $(\mathbb{Z}/4\mathbb{Z})^* = \langle -\overline{1}\rangle \cong C_2$ and $(\mathbb{Z}/8\mathbb{Z})^* = \langle -\overline{1}\rangle \times \langle \overline{5}\rangle \cong C_2 \times C_2$, respectively, where all elements have order dividing 2, hence are solutions of $X^2 \equiv 1 \pmod{2^k}$. Hence let now $k \geq 3$, thus $l = 3$, and we have $(\mathbb{Z}/2^k\mathbb{Z})^* \cong \langle -\overline{1}\rangle \times \langle \overline{5}\rangle \cong C_2 \times C_{2^{k-2}}$.

The set of $\overline{a} \in (\mathbb{Z}/2^k\mathbb{Z})^*$ such that the congruenxce $X^2 \equiv a \pmod{2^k}$ is solvable coincides with the set of squares $\mathcal{Q} \subseteq (\mathbb{Z}/2^k\mathbb{Z})^*$. Considering the cyclic direct factors of $(\mathbb{Z}/2^k\mathbb{Z})^*$ we infer that $\mathcal{Q} = \langle \overline{5}^2\rangle \leq (\mathbb{Z}/2^k\mathbb{Z})^*$ actually is a subgroup, where $|\mathcal{Q}| = |\overline{5}^2| = 2^{k-3}$; note that $5^2 \equiv 1 \pmod{8}$ shows again that all elements of $\mathcal{Q}$ are congruent to 1 modulo 8. We consider the surjective natural map $\nu\colon \mathbb{Z}/2^k\mathbb{Z} \to \mathbb{Z}/8\mathbb{Z}$. Hence we have $|\ker(\nu)| = \frac{2^k}{8} = 2^{k-3}$, implying that there are precisely 2^{k-3} elements $\overline{a} \in \mathbb{Z}/2^k\mathbb{Z}$ such that $a \equiv 1 \pmod{8}$. Thus the latter set coincides with $\mathcal{Q}$, entailing that the congruence $X^2 \equiv a \pmod{2^k}$ is solvable if $a \equiv 1 \pmod{8}$.

Finally, for $\overline{x}, \overline{y} \in (\mathbb{Z}/2^k\mathbb{Z})^*$ we have $\overline{x}^2 = \overline{y}^2$ if and only if $(\overline{x} \cdot \overline{y}^{-1})^2 = \overline{1}$, which holds if and only if $\overline{x} \cdot \overline{y}^{-1} \in \langle -\overline{1}\rangle \times \langle \overline{5}^{2^{k-3}}\rangle \cong C_2 \times C_2$. Hence given solvability the congruence $X^2 \equiv a \pmod{2^k}$ has precisely 4 solutions. ♯

Below, we are going to describe the solvability of the congruence $X^2 \equiv a \pmod{p}$, where $p \in \mathcal{P}$ is odd and $a \in \mathbb{Z}$ such that $p \nmid a$, which is left open in the above considerations. Before doing so, we present an example; note that the congruence $X^2 \equiv 0 \pmod{p}$ is always uniquely solvable modulo p:

Example. We consider the quadratic congruence $X^2 \equiv 453 \pmod{1236}$, actually posed by Gauss. We have $1236 = 2^2 \cdot 3 \cdot 103$, hence by the Chinese remainder theorem this is equivalent to solving the system of quadratic congruences

$$X^2 \equiv 1 \pmod{4}, \quad X^2 \equiv 0 \pmod{3}, \quad X^2 \equiv 41 \pmod{103}.$$

Hence this is more general than the case discussed above, but still we may proceed as follows: The first congruence is equivalent to $X \equiv \pm 1 \pmod{4}$. The second congruence is equivalent to $X \equiv 0 \pmod{3}$, in other words we have $X \equiv \pm 3 \pmod{12}$. For the third congruence, we observe that $41 \equiv 41 + 103 \equiv 144 \equiv 12^2 \pmod{103}$, hence we infer $X \equiv \pm 12 \pmod{103}$. Now the extended Euclidean algorithm entails $1 = \gcd_+(12, 103) = 43 \cdot 12 - 5 \cdot 103$, thus we get $X \equiv \pm 3 \cdot (-5 \cdot 103) \pm 12 \cdot (43 \cdot 12) \equiv \{\pm 297, \pm 321\} \pmod{1236}$.

(12.3) Quadratic residues. Let $p \in \mathcal{P}$ be odd. Then $a \in \mathbb{Z}$ such that $p \nmid a$ is called a **quadratic residue**, if there is $b \in \mathbb{Z}$ such that $\overline{a} = \overline{b}^2 \in (\mathbb{Z}/p\mathbb{Z})^*$, otherwise a is called a **quadratic non-residue**; in other words, a is a quadratic residue if and only if the congruence $X^2 \equiv a \pmod{p}$ is solvable.

Let $\mathcal{Q}_p := \{\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^*; a \in \mathbb{Z} \text{ quadratic residue}\}$ and $\mathcal{N}_p := \{\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^*; a \in \mathbb{Z} \text{ quadratic non-residue}\}$ be the sets of squares and non-squares in $(\mathbb{Z}/p\mathbb{Z})^*$, respectively. For $a \in \mathbb{Z}$ such that $p \nmid a$ let the **Legendre symbol** be defined as $\left(\frac{a}{p}\right) := 1$ if $\overline{a} \in \mathcal{Q}_p$, and $\left(\frac{a}{p}\right) := -1$ if $\overline{a} \in \mathcal{N}_p$; we let $\left(\frac{a}{p}\right) := 0$ if $p \mid a$.

Note that $\left(\frac{\cdot}{p}\right)$ only depends on residue classes, hence we may also write $\left(\frac{\overline{a}}{p}\right)$. In this sense, recalling that $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic of even order $p-1$, if $\rho \in \mathbb{Z}$ is a primitive root modulo p, then $\left(\frac{\cdot}{p}\right)$ coincides with the surjective natural group homomorphism $(\mathbb{Z}/p\mathbb{Z})^* \to \{\pm 1\} \colon \overline{\rho}^i \mapsto (-1)^i$. This entails:

Proposition: Euler criterion. (Legendre symbols are determined in $\mathbb{Z}/p\mathbb{Z}$.) For any $a \in \mathbb{Z}$ such that $p \nmid a$ we have $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

Proof. If $\left(\frac{\overline{a}}{p}\right) = 1$, then $\overline{a}^{\frac{p-1}{2}} = \overline{1} \in (\mathbb{Z}/p\mathbb{Z})^*$; if $\left(\frac{\overline{a}}{p}\right) = -1$, then since $-\overline{1} \in (\mathbb{Z}/p\mathbb{Z})^*$ is the unique element of order 2, we have $\overline{a}^{\frac{p-1}{2}} = -\overline{1} \in (\mathbb{Z}/p\mathbb{Z})^*$. ♯

Example. For $p := 3$ we get $\mathcal{Q}_3 = \{\overline{1}\}$ and $\mathcal{N}_3 = \{-\overline{1}\}$; for $p := 5$ we get $\mathcal{Q}_5 = \{\pm\overline{1}\}$ and $\mathcal{N}_5 = \{\pm\overline{2}\}$; for $p := 7$ we get $\mathcal{Q}_7 = \{\overline{1}, \overline{2}, \overline{4}\}$ and $\mathcal{N}_7 = \{-\overline{1}, -\overline{2}, -\overline{4}\}$.

(12.4) The quadratic reciprocity law. In order to compute Legendre symbols $\left(\frac{a}{p}\right)$, by factoring $a \in \mathbb{Z}$ and using the multiplicatiivity of $\left(\frac{\cdot}{p}\right)$, it suffices to be able to determine $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$, as well as $\left(\frac{q}{p}\right)$, where $q \in \mathcal{P}$ is odd such that $q \neq p$; recall that to find $\left(\frac{a}{p}\right)$ we might as well compute $\left(\frac{b}{p}\right)$ for any $b \equiv a \pmod{p}$. We now proceed to the famous quadratic reciprocity law, whose main part is to relate $\left(\frac{q}{p}\right)$ to $\left(\frac{p}{q}\right)$, that is to compare the quadratic residuosity properties of distinct odd primes.

Theorem: Quadratic reciprocity law [Gauss, 1796]**.** Let $p \in \mathcal{P}$ be odd.

a) Let $q \in \mathcal{P}$ be odd such that $q \neq p$. Then we have $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$.

In other words, if $p \equiv 1 \pmod{4}$ or $q \equiv 1 \pmod{4}$ then we have $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$, while if both $p, q \equiv 3 \pmod{4}$ then we have $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$.

b) '2. Ergänzungssatz'. We have $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

In other words, we have $2 \in \mathcal{Q}_p$ if and only if $p \equiv \pm 1 \pmod 8$.

c) '1. Ergänzungssatz'. We have $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

In other words, we have $-1 \in \mathcal{Q}_p$ if and only if $p \equiv 1 \pmod 4$.

Proof. Note first that c) is just the Euler criterion applied to $a := -1$; alternatively, as a consequence of Artin's Theorem, the quadratic congruence $X^2 \equiv -1 \pmod p$ is solvable if and only if $p \equiv 1 \pmod 4$.

Moreover, for the reformulation of b) note that since $(\mathbb{Z}/8\mathbb{Z})^* \cong \langle -\overline{1}\rangle \times \langle \overline{5}\rangle \cong C_2 \times C_2$ we have $p^2 \equiv 1 \pmod 8$ for any p, where from $(\mathbb{Z}/16\mathbb{Z})^* \cong \langle -\overline{1}\rangle \times \langle \overline{5}\rangle \cong C_2 \times C_4$ we conclude that $p^2 \equiv 1 \pmod{16}$ if and only if $\overline{p} \in \langle -\overline{1}\rangle \times \langle \overline{5}^2\rangle$, that is $p \equiv \{\pm 1, \pm 7\} \pmod{16}$, in other words $p \equiv \pm 1 \pmod 8$.

To prove the main assertions a) and b) we proceed in a series of steps: Following EISENSTEIN, let $\mathcal{H}_p := 1 + \mathbb{Z}_{\frac{p-1}{2}} = \{1, \ldots, \frac{p-1}{2}\}$. Then any $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^*$ can be written uniquely as $\overline{a} = \overline{\epsilon}_a \overline{\alpha}$, where $\epsilon_a \in \{\pm 1\}$ and $\alpha \in \mathcal{H}_p$.

i) Let $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^*$, and for $i \in \mathcal{H}_p$ let $\overline{a}\overline{i} = \overline{\epsilon}_i \overline{\alpha}_i$, where $\epsilon_i \in \{\pm 1\}$ and $\alpha_i \in \mathcal{H}_p$. Then we have the **Gauss Lemma** saying that $\left(\frac{a}{p}\right) = \prod_{i \in \mathcal{H}_p} \epsilon_i$:

We first show that the α_i, for $i \in \mathcal{H}_p$, are pairwise distinct: Let $\alpha_i = \alpha_j$ for $i, j \in \mathcal{H}_p$, then we have $\overline{a}^2\overline{i}^2 = \overline{\alpha}_i^2 = \overline{\alpha}_j^2 = \overline{a}^2\overline{j}^2 \in (\mathbb{Z}/p\mathbb{Z})^*$, hence $\overline{i}^2 = \overline{j}^2$, that is $\overline{i}^2\overline{j}^{-2} = \overline{1}$, hence $\overline{i}\overline{j}^{-1} = \pm\overline{1}$, that is $\overline{i} = \pm\overline{j}$, which finally implies $\overline{i} = \overline{j}$.

Thus we have $\overline{a}^{\frac{p-1}{2}} \cdot \prod_{i \in \mathcal{H}_p} \overline{i} = \prod_{i \in \mathcal{H}_p} \overline{a}\overline{i} = \prod_{i \in \mathcal{H}_p} \overline{\epsilon}_i \overline{\alpha}_i = \prod_{i \in \mathcal{H}_p} \overline{\epsilon}_i \cdot \prod_{i \in \mathcal{H}_p} \overline{\alpha}_i = \prod_{i \in \mathcal{H}_p} \overline{\epsilon}_i \cdot \prod_{i \in \mathcal{H}_p} \overline{i} \in (\mathbb{Z}/p\mathbb{Z})^*$, thus $\left(\frac{a}{p}\right) = \overline{a}^{\frac{p-1}{2}} = \prod_{i \in \mathcal{H}_p} \overline{\epsilon}_i$. ♯

ii) Using the notation introduced above, for $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^*$ and $i \in \mathcal{H}_p$ let $ai = \epsilon_i\alpha_i + e_ip$, where $e_i \in \mathbb{Z}$. Now, if $\epsilon_i = 1$, then we have $2ai = 2\alpha_i + 2e_ip$, hence $\frac{2ai}{p} = \frac{2\alpha_i}{p} + 2e_i$, thus $\lfloor \frac{2ai}{p} \rfloor = 2e_i$ is even. If $\epsilon_i = -1$, then we have $2ai = -2\alpha_i + 2e_ip$, hence $\frac{2ai}{p} = -\frac{2\alpha_i}{p} + 2e_i$, thus $\lfloor \frac{2ai}{p} \rfloor = 2e_i - 1$ is odd.

In conclusion $\epsilon_i = (-1)^{\lfloor \frac{2ai}{p} \rfloor}$, thus $\left(\frac{a}{p}\right) = \prod_{i \in \mathcal{H}_p} (-1)^{\lfloor \frac{2ai}{p} \rfloor} = (-1)^{\sum_{i \in \mathcal{H}_p} \lfloor \frac{2ai}{p} \rfloor}$.

iii) Now let $a \in \mathbb{Z}$ be odd such that $p \nmid a$. Then, using $\left(\frac{4}{p}\right) = \left(\frac{2^2}{p}\right) = \left(\frac{2}{p}\right)^2 = 1$, we get $\left(\frac{2a}{p}\right) = \left(\frac{2a+2p}{p}\right) = \left(\frac{4 \cdot \frac{a+p}{2}}{p}\right) = \left(\frac{4}{p}\right) \cdot \left(\frac{\frac{a+p}{2}}{p}\right) = \left(\frac{\frac{a+p}{2}}{p}\right)$. This yields $\left(\frac{2a}{p}\right) = (-1)^{\sum_{i \in \mathcal{H}_p} \lfloor \frac{i(a+p)}{p} \rfloor} = (-1)^{\sum_{i \in \mathcal{H}_p} (i + \lfloor \frac{ia}{p} \rfloor)} = (-1)^{\sum_{i \in \mathcal{H}_p} i} \cdot (-1)^{\sum_{i \in \mathcal{H}_p} \lfloor \frac{ia}{p} \rfloor}$.

The sum formula for arithmetic series yields $\sum_{i \in \mathcal{H}_p} i = \sum_{i=1}^{\frac{p-1}{2}} i = \binom{\frac{p+1}{2}}{2} = \frac{(p-1)(p+1)}{8} = \frac{p^2-1}{8}$, hence we get $\left(\frac{2a}{p}\right) = (-1)^{\frac{p^2-1}{8}} \cdot (-1)^{\sum_{i \in \mathcal{H}_p} \lfloor \frac{ia}{p} \rfloor}$.

In particular, for $a := 1$ we get $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \cdot (-1)^{\sum_{i \in \mathcal{H}_p} \lfloor \frac{i}{p} \rfloor} = (-1)^{\frac{p^2-1}{8}}$, proving b). Thus, from $\left(\frac{2a}{p}\right) = \left(\frac{2}{p}\right) \cdot \left(\frac{a}{p}\right)$ we get $\left(\frac{a}{p}\right) = (-1)^{\sum_{i \in \mathcal{H}_p} \lfloor \frac{ia}{p} \rfloor}$.

iv) Let now $q \in \mathcal{P}$ be odd such that $q \neq p$. Letting $\mathcal{H} := \mathcal{H}_p \times \mathcal{H}_q$, we consider $\sigma := |\{[i,j] \in \mathcal{H}; qi > pj\}|$ and $\tau := |\{[i,j] \in \mathcal{H}; qi < pj\}|$. Since $p \nmid qi$ and $q \nmid pj$, we have $qi \neq pj$ anyway, and thus $\sigma + \tau = |\mathcal{H}| = \frac{p-1}{2} \cdot \frac{q-1}{2}$.

For $i \in \mathcal{H}_p$ we have $\frac{qi}{p} \leq \frac{q(p-1)}{2p} < \frac{q}{2}$, hence $\lfloor \frac{qi}{p} \rfloor \leq \frac{q-1}{2}$. Thus for $j \in \mathcal{H}_q$ we have $qi > pj$ if and only if $j \leq \lfloor \frac{qi}{p} \rfloor$, hence we get $\sigma = \sum_{i \in \mathcal{H}_p} \lfloor \frac{qi}{p} \rfloor$. By symmetry, we also have $\tau = \sum_{j \in \mathcal{H}_q} \lfloor \frac{pj}{q} \rfloor$. This finally entails $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\sum_{j \in \mathcal{H}_q} \lfloor \frac{pj}{q} \rfloor} \cdot (-1)^{\sum_{i \in \mathcal{H}_p} \lfloor \frac{qi}{p} \rfloor} = (-1)^{\sigma+\tau} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$, proving a). ♯

The quadratic reciprocity law allows to compute Legendre symbols straightforwardly, and thus to decide the solvability of quadratic congruences with respect to odd prime moduli quickly; but note that this does not provide the solutions:

Example. We have $\left(\frac{17}{19}\right) = \left(\frac{19}{17}\right) = \left(\frac{2}{17}\right) = 1$, and $\left(\frac{21}{23}\right) = \left(\frac{3}{23}\right) \cdot \left(\frac{7}{23}\right) = (-1)^2 \cdot \left(\frac{23}{3}\right) \cdot \left(\frac{23}{7}\right) = \left(\frac{-1}{3}\right) \cdot \left(\frac{2}{7}\right) = \left(\frac{-1}{3}\right) \cdot \left(\frac{2}{7}\right) = (-1) \cdot 1 = -1$, as well as $\left(\frac{41}{103}\right) = \left(\frac{103}{41}\right) = \left(\frac{21}{41}\right) = \left(\frac{3}{41}\right) \cdot \left(\frac{7}{41}\right) = \left(\frac{41}{3}\right) \cdot \left(\frac{41}{7}\right) = \left(\frac{-1}{3}\right) \cdot \left(\frac{-1}{7}\right) = (-1) \cdot (-1) = 1$.

13 Applications

(13.1) Primes in arithmetic progressions. We consider arbitrary moduli $n \in \mathbb{N}$. Then for any prime $p \in \mathbb{Z}$ we have either $p \mid n$ or $\overline{p} \in (\mathbb{Z}/n\mathbb{Z})^*$. Hence, given $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$, we ask ourselves, kind of conversely, whether there are infinitely many primes $p \in \mathcal{P}$ such that $\overline{p} = \overline{a}$.

The following refers to the cases $n = 4$ and $n = 3$, respectively, where in both cases the first part is seen straightforwardly, while the second part follows from the quadratic reciprocity law.

Proposition. a) There are infinitely many $p \in \mathcal{P}$ such that $p \equiv -1 \pmod 4$.

b) There are infinitely many $p \in \mathcal{P}$ such that $p \equiv 1 \pmod 4$.

Proof. a) Assume to the contrary that $\{p_1, \ldots, p_r\}$, for some $r \in \mathbb{N}$, are all the primes $p \in \mathcal{P}$ such that $p \equiv -1 \pmod 4$. Then let $z := -1 + 4 \cdot \prod_{i=1}^r p_i \in \mathbb{Z}$, hence $z \equiv -1 \pmod 4$. But for any $q \in \mathcal{P}$ such that $q \mid z$, by construction we have $q \equiv 1 \pmod 4$, hence we have $z \equiv 1 \pmod 4$ as well, a contradiction.

b) Assume to the contrary that $\{p_1, \ldots, p_r\}$, for some $r \in \mathbb{N}$, are all the primes $p \in \mathcal{P}$ such that $p \equiv 1 \pmod 4$. Then let $z := 1 + 4 \cdot \prod_{i=1}^r p_i^2 \in \mathbb{Z}$, and let $q \in \mathcal{P}$ such that $q \mid z$. Then by construction we have $q \equiv -1 \pmod 4$. But $-1 \equiv (2 \cdot \prod_{i=1}^r p_i)^2 \pmod q$ shows that $q \equiv 1 \pmod 4$, a contradiction. ♯

Proposition. a) There are infinitely many $p \in \mathcal{P}$ such that $p \equiv -1 \pmod 3$.

b) There are infinitely many $p \in \mathcal{P}$ such that $p \equiv 1 \pmod 3$.

Proof. a) Assume to the contrary that $\{p_1, \ldots, p_r\}$, for some $r \in \mathbb{N}$, are all the primes $p \in \mathcal{P}$ such that $p \equiv -1 \pmod 3$. Then let $z := -1 + 3 \cdot \prod_{i=1}^{r} p_i \in \mathbb{Z}$, hence $z \equiv -1 \pmod 3$. But for any $q \in \mathcal{P}$ such that $q \mid z$, by construction we have $q \equiv 1 \pmod 3$, hence we have $z \equiv 1 \pmod 3$ as well, a contradiction.

b) Assume to the contrary that $\{p_1, \ldots, p_r\}$, for some $r \in \mathbb{N}$, are all the primes $p \in \mathcal{P}$ such that $p \equiv 1 \pmod 3$. Then let $z := 3 + 4 \cdot \prod_{i=1}^{r} p_i^2 \in \mathbb{Z}$, and let $q \in \mathcal{P}$ such that $q \mid z$. Then by construction we have $q \equiv -1 \pmod 3$, hence $\left(\frac{q}{3}\right) = \left(\frac{-1}{3}\right) = -1$. But $-3 \equiv (2 \cdot \prod_{i=1}^{r} p_i)^2 \pmod q$ shows that $1 = \left(\frac{-3}{q}\right) = \left(\frac{-1}{q}\right) \cdot \left(\frac{3}{q}\right) = (-1)^{\frac{q-1}{2}} \cdot (-1)^{\frac{q-1}{2}} \cdot \left(\frac{q}{3}\right) = \left(\frac{q}{3}\right)$, a contradiction. ♯

The following deep theorem (which is not proved here) provides an affirmative answer to the question whether there are are infinitely many primes $p \in \mathcal{P}$ such that $\overline{p} = \overline{a}$, for some fixed $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$. Actually, the precise answer uses the prime number function $\pi(x) := |\mathcal{P}_{\leq x}|$, for $x \in \mathbb{R}_{>0}$:

Theorem: Dirichlet [1837]. Let $n \in \mathbb{N}$ and $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$. Then we have

$$\lim_{x \to \infty} \frac{|\{p \in \mathcal{P}_{\leq x}; p \equiv a \pmod n\}|}{\pi(x)} = \frac{1}{|(\mathbb{Z}/n\mathbb{Z})^*|}.$$

Hence there are infinitely many primes $p \in \mathbb{Z}$ such that $p \equiv a \pmod n$. ♯

(13.2) Varying prime moduli. We change the point of view, fix $a \in \mathbb{Z}$, and let the modulus $p \in \mathcal{P}$, being odd such that $p \nmid a$, vary. We ask ourselves whether there are infinitely many odd primes such that a is a quadratic residue and a quadratic non-residue modulo p, respectively.

Theorem. Let $0 \neq a \in \mathbb{Z}$. Then there are infinitely many odd primes $p \in \mathcal{P}$ such that $p \nmid a$ and $\left(\frac{a}{p}\right) = 1$.

Proof. Assume to the contrary that $\{p_1, \ldots, p_r\}$, for some $r \in \mathbb{N}_0$, are all odd primes $p \in \mathcal{P}$ such that $p \nmid a$ and $\left(\frac{a}{p}\right) = 1$. Let $b \in \mathbb{Z}$ such that $\gcd_+(a, b) = 1$ and $2 \mid ab$, chosen large enough such that $z := \left(b \cdot \prod_{i=1}^{r} p_i\right)^2 - a > 1$; note that here we need $a \neq 0$. Then $\gcd_+(a, b \cdot \prod_{i=1}^{r} p_i) = 1$ entails $\gcd_+(z, ab \cdot \prod_{i=1}^{r} p_i) = 1$. Let $q \in \mathcal{P}$ such that $q \mid z$, then by construction q is odd such that $\left(\frac{a}{p}\right) = -1$. But $a \equiv (b \cdot \prod_{i=1}^{r} p_i)^2 \pmod q$ shows that $\left(\frac{a}{q}\right) = 1$, a contradiction. ♯

Theorem. Let $a \in \mathbb{Z}$ be not a square. Then there are infinitely many odd primes $p \in \mathcal{P}$ such that $p \nmid a$ and $\left(\frac{a}{p}\right) = -1$.

Proof. By the multiplicativity of $\left(\frac{\cdot}{p}\right)$ we may assume that $a \in \mathbb{Z} \setminus \{0,1\}$ is squarefree. We first consider some exeptional small cases:

i) Let $a := -1$. Then for an odd prime $p \in \mathcal{P}$ we have $\left(\frac{-1}{p}\right) = -1$ if and only if $p \equiv -1 \pmod 4$, of which we already know that there are infinitely many.

ii) Let $a := 2$. Then for an odd prime $p \in \mathcal{P}$ we have $\left(\frac{2}{p}\right) = 1$ if and only if $p \equiv \pm 1 \pmod 8$. Hence assume to the contrary that $\{3\} \dot\cup \{p_1, \ldots, p_r\}$, for some $r \in \mathbb{N}_0$, are all the odd primes $p \in \mathcal{P}$ such that $p \equiv \pm 3 \pmod 8$. Then let $z := 3 + 8 \cdot \prod_{i=1}^r p_i \in \mathbb{Z}$, hence in particular $z \equiv 3 \pmod 8$. But for any $q \in \mathcal{P}$ such that $q \mid z$, by construction we have $q \equiv \pm 1 \pmod 8$, hence we have $z \equiv \pm 1 \pmod 8$ as well, a contradiction.

iii) Let $a := -2$. Then for an odd prime $p \in \mathcal{P}$ we have $1 = \left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{2}{p}\right)$ if and only if $p \equiv 1 \pmod 4$ and $p \equiv \pm 1 \pmod 8$, or $p \equiv -1 \pmod 4$ and $p \equiv \pm 3 \pmod 8$, that is $p \equiv 1 \pmod 8$ or $p \equiv 3 \pmod 8$.

Hence assume to the contrary that $\{5\} \dot\cup \{p_1, \ldots, p_r\}$, for some $r \in \mathbb{N}_0$, are all the odd primes $p \in \mathcal{P}$ such that $p \equiv -1 \pmod 8$ or $p \equiv -3 \pmod 8$. Then let $z := 5 + 8 \cdot \prod_{i=1}^r p_i \in \mathbb{Z}$, hence in particular $z \equiv -3 \pmod 8$. But for any $q \in \mathcal{P}$ such that $q \mid z$, by construction we have $q \equiv 1 \pmod 8$ or $q \equiv 3 \pmod 8$, hence we have $z \equiv 1 \pmod 8$ or $z \equiv 3 \pmod 8$ as well, a contradiction.

iv) Hence we may now assume that $a = (-1)^\epsilon \cdot 2^e \cdot \prod_{j=1}^s q_j$, where $q_i \in \mathcal{P}$ are pairwise distinct odd primes, for some $s \in \mathbb{N}$, and $\epsilon, e \in \{0,1\}$. Assume to the contrary that $\{p_1, \ldots, p_r\}$, for some $r \in \mathbb{N}_0$, are all the odd primes $p \in \mathcal{P}$ such that $p \nmid a$ and $\left(\frac{a}{p}\right) = -1$. Then we have $p_i \neq q_j$ for all $i \in \{1, \ldots, r\}$ and $j \in \{1, \ldots, s\}$. Hence, letting $x \in \mathbb{Z}$ such that $\overline{x} \in \mathcal{N}_{q_s}$, by the Chinese remainder theorem let $z \in \mathbb{N}$ such that

$$\begin{aligned} z &\equiv 1 \pmod 8, & z &\equiv 1 \pmod{p_i} & &\text{for all } i \in \{1, \ldots, r\}, \\ z &\equiv x \pmod{q_s}, & z &\equiv 1 \pmod{q_j} & &\text{for all } j \in \{1, \ldots, s-1\}. \end{aligned}$$

Letting $z = \prod_{k=1}^t l_k$, where $l_k \in \mathcal{P}$ and $t \in \mathbb{N}$, we have $l_k \neq 2$ and $l_k \neq p_i$ and $l_k \neq q_j$, for all $k \in \{1, \ldots, t\}$ and $i \in \{1, \ldots, r\}$ and $j \in \{1, \ldots, s\}$. Hence we get $\prod_{k=1}^t \left(\frac{a}{l_k}\right) = \prod_{k=1}^t \left(\frac{-1}{l_k}\right)^\epsilon \cdot \prod_{k=1}^t \left(\frac{2}{l_k}\right)^e \cdot \prod_{k=1}^t \prod_{j=1}^s \left(\frac{q_j}{l_k}\right)$.

Since $z \equiv 1 \pmod 4$, and $l_k \equiv \pm 1 \pmod 4$, we infer that $l_k \equiv -1 \pmod 4$ for an even number of $k \in \{1, \ldots, t\}$. Since $\left(\frac{-1}{l_k}\right) = 1$ if and only if $l_k \equiv 1 \pmod 4$, we conclude that $\prod_{k=1}^t \left(\frac{-1}{l_k}\right) = 1$. Similarly, since $z \equiv 1 \pmod 8$, and $l_k \equiv \pm 1 \pmod 8$ or $l_k \equiv \pm 3 \pmod 8$, where $(\pm 3)^2 \equiv 1 \pmod 8$, we infer that $l_k \equiv \pm 3 \pmod 8$ for an even number of $k \in \{1, \ldots, t\}$. Since $\left(\frac{2}{l_k}\right) = 1$ if and only if $l_k \equiv \pm 1 \pmod 8$, we conclude that $\prod_{k=1}^t \left(\frac{2}{l_k}\right) = 1$.

Since $\left(\frac{q_j}{l_k}\right) = \left(\frac{l_k}{q_j}\right)$ whenever $l_k \equiv 1 \pmod 4$, while $\left(\frac{q_j}{l_k}\right) = \pm \left(\frac{l_k}{q_j}\right)$ whenever

$l_k \equiv -1 \pmod 4$, which happens for an even number of $k \in \{1, \dots, t\}$, for fixed $j \in \{1, \dots, s\}$ we get $\prod_{k=1}^{t} \left(\frac{q_j}{l_k}\right) = \prod_{k=1}^{t} \left(\frac{l_k}{q_j}\right)$. Thus in conclusion we have $\prod_{k=1}^{t} \left(\frac{a}{l_k}\right) = \prod_{j=1}^{s} \prod_{k=1}^{t} \left(\frac{l_k}{q_j}\right) = \prod_{j=1}^{s} \left(\frac{z}{q_j}\right) = \left(\frac{x}{q_s}\right) \cdot \prod_{j=1}^{s-1} \left(\frac{z}{q_j}\right) = -1$. Hence there is $k \in \{1, \dots, t\}$ such that $\left(\frac{a}{l_k}\right) = -1$, a contradiction. ♯

(13.3) Example: Fermat numbers. Finally, we consider the Fermat numbers $F_n := 2^{2^n} + 1 \in \mathbb{N}$, for $n \in \mathbb{N}_0$, again. The following, due to Lucas, is one of the few general properties known to hold for prime divisors of F_n:

Lemma. Let $n \geq 2$, and $p \in \mathcal{P}$ such that $p \mid F_n$. Then we have $2^{n+2} \mid p - 1$.

Proof. Note that p is odd. For $\overline{2} \in (\mathbb{Z}/p\mathbb{Z})^*$ we have $\overline{2}^{2^n} = -\overline{1}$, hence $\overline{2}^{2^{n+1}} = \overline{1}$. This implies that $\overline{2} \in (\mathbb{Z}/p\mathbb{Z})^*$ has order 2^{n+1}, from which we infer $2^{n+1} \mid p-1$. Thus, since $n \geq 2$, we have $p \equiv 1 \pmod 8$. Hence we have $\left(\frac{2}{p}\right) = 1$ and there is $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^*$ such that $\overline{a}^2 = \overline{2}$. Hence we have $\overline{a}^{2^{n+2}} = (\overline{a}^2)^{2^{n+1}} = \overline{2}^{2^{n+1}} = \overline{1}$. Assume that $\overline{a}^{2^{n+1}} = \overline{1}$, then $-\overline{1} = \overline{2}^{2^n} = (\overline{a}^2)^{2^n} = \overline{a}^{2^{n+1}} = \overline{1}$, a contradiction. Hence we have $\overline{a}^{2^{n+1}} \neq \overline{1}$; thus actually necessarily $\overline{a}^{2^{n+1}} = -\overline{1}$, but we do not need that. This implies that $\overline{a}$ has order 2^{n+2}, which entails $2^{n+2} \mid p - 1$. ♯

Applying this for $n \in \{2, 3, 4\}$ shows that it a fairly weak statement: For $n = 2$ we have $2^{2+2} = 16$, hence we get $p = 17 = 2^4 + 1 = F_2$. For $n = 3$ we have $2^{3+2} = 32$, hence we get $p \in \mathcal{P} \cap \{32 \cdot k + 1; k \in \{1, \dots, 8\}\} = \{97, 193, 257\}$, where $F_3 = 2^8 + 1 = 257$. For $n = 4$ we have $2^{4+2} = 64$, hence we get $p \in \mathcal{P} \cap \{64 \cdot k + 1; k \in \{1, \dots, 2^{10}\}\} = \{193, 257, \dots, 65537\}$, a set of cardinality 210, where $F_4 = 2^{16} + 1 = 65537$.

Still, in rare cases, see Table 10, it is helpful to discover small prime divisors of F_n explicitly, by running through the numbers $p := 2^{n+2} \cdot k + 1 \in \mathbb{N}$, for smallish $k \in \mathbb{N}$, and checking whether p divides F_n; in this case p is a prime. We also indicate the 2-parts of the numbers $p - 1$ found, which may indeed exceed $n + 2$. Finally, the decomposability or primality of the co-factors remaining after dividing out the prime divisors found can be checked using the Fermat decomposability test or the Lucas primality test, respectively, see (14.3).

14 Primality testing

(14.1) Fermat test. Letting $1 \neq n \in \mathbb{N}$, we aim to decide algorithmically whether n is a prime or decomposable, but without actually computing the factorisation of n. To do so, recall that n is a prime if and only if $\varphi(n) = n - 1$, where in this case the group of prime residues $(\mathbb{Z}/n\mathbb{Z})^* \cong C_{n-1}$ is cyclic.

a) Without actually determining $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$, we may proceed as follows: If n is a prime, then Euler's Theorem implies $\overline{a}^{n-1} = \overline{1}$, for all $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$.

Table 10: Prime divisors of Fermat numbers.

n	2^{n+2}	k	p	$\nu_2(p-1)$	co-factor prime?
5	128	5	641	7	yes
6	256	1071	274177	8	yes
9	2048	1184	2424833	16	no
10	4096	11131	45592577	12	
		1583748	6487031809	14	no
11	8192	39	319489	13	
		119	974849	13	no
12	16384	7	114689	14	
		1588	26017793	16	
		3892	63766529	16	no

Hence we have the **Fermat decomposability test**, saying that if if there is $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$ such that $\overline{a}^{n-1} \neq \overline{1}$, then n is decomposable; in this case $\overline{a}$ is called a **Fermat decomposability witness** for n.

But this does not provide a primality test: If n is decomposable, but still $\overline{a}^{n-1} = \overline{1}$ for some $\overline{1} \neq \overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$, then n is called a **Fermat pseudo-prime** with respect to the **base** $\overline{a}$, which is called a **Fermat liar** for n. If n is a Fermat pseudo-prime with respect to all bases $\overline{1} \neq \overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$, then n is called a **Carmichael number** [Korselt, 1899; Carmichael, 1910]. These are precisely the decomposable numbers escaping the Fermat decomposability test.

Example. i) We consider $2^{12} + 1 = 4097 = 17 \cdot 241$. Then we have $\overline{2} \in (\mathbb{Z}/4097\mathbb{Z})^*$, and letting $a := 2$ we get $2^{12} \equiv -1 \pmod{4097}$, hence $2^{24} \equiv 1 \pmod{4097}$, and $4096 = 170 \cdot 24 + 16$ yields $2^{4096} \equiv (2^{24})^{170} \cdot 2^{16} \equiv 2^{12} \cdot 2^4 \equiv -16 \not\equiv 1 \pmod{4097}$. Hence $\overline{2}$ is a Fermat decomposability witness for 4097.

ii) We have $561 = 3 \cdot 11 \cdot 17$, hence $(\mathbb{Z}/561\mathbb{Z})^* \cong (\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/11\mathbb{Z})^* \times (\mathbb{Z}/17\mathbb{Z})^* \cong C_2 \times C_{10} \times C_{16}$, implies that for all $\overline{a} \in (\mathbb{Z}/561\mathbb{Z})^*$ we have $\overline{a}^{\mathrm{lcm}_+(2,10,16)} = \overline{1}$, where $\mathrm{lcm}_+(2, 10, 16) = 80 \mid 560 = 561 - 1$; thus 561 is a Carmichael number. The Carmichael numbers $\leq 10^4$ are $\{561, 1105, 1729, 2465, 2821, 6601, 8911\}$.

b) Hence the question arises, how many Carmichael numbers there are. Indeed, there are infinitely many of them, where more precisely we have the estimates $n^{\frac{2}{7}} \leq |\{k \in \{1, \ldots, n\}; k \text{ Carmichael number}\}| \leq n^{1-(1+\epsilon)\cdot \frac{\ln(\ln(\ln(n)))}{\ln(\ln(n))}}$, for $n \to \infty$ and for all $\epsilon > 0$ [Alford-Granville-Pomerance, 1992; Pomerance-Selfridge-Wagstaff, 1980].

Still, the set $U_n := \{\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*; \overline{a}^{n-1} = \overline{1}\} \leq (\mathbb{Z}/n\mathbb{Z})^*$ is a subgroup, where we have $U_n = (\mathbb{Z}/n\mathbb{Z})^*$ if and only if n is either a prime or a Carmichael number. If $U_n < (\mathbb{Z}/n\mathbb{Z})^*$, then by Lagrange's Theorem we have $\frac{|U_n|}{|(\mathbb{Z}/n\mathbb{Z})^*|} \leq \frac{1}{2}$, implying

that the fraction of Fermat liars is at most $\frac{1}{2}$. Hence we have the following **randomised** algorithm to decide decomposability:

Given an error bound $0 < \epsilon \leq \frac{1}{2}$, for at least $\lceil -\log_2(\epsilon) \rceil$ randomly chosen elements of $(\mathbb{Z}/n\mathbb{Z})^*$ we perform the Fermat decomposability test; if a Fermat decomposability witness is found then 'decomposable' is returned, otherwise 'prime' (or 'probably prime or Carmichael', to be precise) is returned. Thus this is a **Monte-Carlo** algorithm insasmuch the answer 'decomposable' is correct, while the answer 'prime' is incorrect with an error probability of at most ϵ.

(14.2) Lucas test. Let still $1 \neq n \in \mathbb{N}$. The **Lucas primality test [1876]** aims at proving that $(\mathbb{Z}/n\mathbb{Z})^*$ is cyclic of order $n-1$, by exhibiting an element $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$ of order $n-1$. The latter property is verified, letting $p_1, \ldots, p_r \in \mathcal{P}$ be the prime divisors of $n-1$ for some $r \in \mathbb{N}_0$, by checking whether $\overline{a}^{n-1} = \overline{1}$ and $\overline{a}^{\frac{n-1}{p_i}} \neq \overline{1}$, for all $i \in \{1, \ldots, r\}$.

If n is a prime, then the tuple $[a; p_1, \ldots, p_r]$ is a called a **Lucas primality certificate** for n, where the primitive root $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$ is called a **Lucas primality witness**. But to achieve this we need to apply a factorisation algorithm to $n-1$, and to apply the Lucas primality test recursively to verify primality of the prime factors of $n-1$ found. Unfortunately, no 'fast' (more precisely, polynomial) factorisation algorithm is known.

This finally yields a **Pratt primality certificate [1975]** for n, consisting of a Lucas primality certificate for n, together with Pratt primality certificates for the prime factors of $n-1$; note that the recursion is anchored by the empty Lucas primality certificate $[2;]$ for $n = 2$. In terms of complexity theory of algorithms a Pratt primality certificate for n is a **polynomial certificate** for primality of n, saying that using this primality of n can be verified algorithmically needing computing time which is polynomial in the input size $\ln(n)$. Similarly, providing a proper divisor of n is a polynomial certificate for decomposability of n.

(14.3) Example: Fermat numbers. We consider the Fermat numbers $F_n := 2^{2^n} + 1 \in \mathbb{N}$, for $n \in \mathbb{N}_0$, again. The Fermat decomposability test amounts to finding $\overline{a} \in (\mathbb{Z}/F_n\mathbb{Z})^*$ such that $a^{F_n - 1} \equiv a^{2^{2^n}} \not\equiv 1 \pmod{F_n}$, while the Lucas primality test amounts to finding $\overline{a} \in (\mathbb{Z}/F_n\mathbb{Z})^*$ such that $a^{\frac{F_n-1}{2}} \equiv a^{2^{2^n}-1} \not\equiv 1 \pmod{F_n}$ and $a^{F_n-1} \equiv a^{2^{2^n}} \equiv 1 \pmod{F_n}$. Actually, we can do better:

Lemma: Pepin's test [1877]. Let $n \geq 1$. Then we have $3 \nmid F_n$, and F_n is a prime if and only if $3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$.

Proof. We have $F_n \equiv (-1)^{2^n} + 1 \equiv -1 \pmod{3}$, hence $\overline{3} \in (\mathbb{Z}/F_n\mathbb{Z})^*$. Now let F_n be a prime; then since $F_n \equiv 2^{2^n} + 1 \equiv 1 \pmod{4}$ we have $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right) = \left(\frac{-1}{3}\right) = -1$, hence the Euler criterion yields $3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$. Conversely,

let $3^{\frac{F_n-1}{2}} \equiv 3^{2^{2^n}-1} \equiv -1 \pmod{F_n}$, hence $3^{F_n-1} \equiv 3^{2^{2^n}} \equiv 1 \pmod{F_n}$, thus $\overline{3} \in (\mathbb{Z}/F_n\mathbb{Z})^*$ has order $2^{2^n} = F_n - 1$, implying that F_n is a prime. ♯

Hence the second part of the above argument shows that, if F_n is a prime then 3 is a Lucas primality witness.

Now the Fermat numbers $F_1 = 2^2+1 = 5$, $F_2 = 2^4+1 = 17$, $F_3 = 2^8+1 = 257$, $F_4 = 2^{16}+1 = 65537$ are seen to be primes as follows, letting $a := 3$: For $n = 1$ we get $3^{\frac{F_1-1}{2}} \equiv 3^2 \equiv 9 \equiv -1 \pmod{F_1}$; for $n = 2$ we successively compute $3^2 \equiv 9 \pmod{F_2}$ and $3^4 \equiv 81 \equiv -4 \pmod{F_2}$ and $3^{\frac{F_2-1}{2}} \equiv 3^8 \equiv 4^2 \equiv -1 \pmod{F_2}$; similarly, sparing the details, for $n = 3$ we get $3^{\frac{F_3-1}{2}} \equiv 3^{128} \equiv -1 \pmod{F_3}$; and for $n = 4$ we get $3^{\frac{F_4-1}{2}} \equiv 3^{32768} \equiv -1 \pmod{F_4}$.

To the contrary, for $F_5 = 2^{32}+1 = 4\,294\,967\,297$ we get $3^{\frac{F_5-1}{2}} \equiv 10\,324\,303 \not\equiv -1 \pmod{F_5}$, implying that F_5 is not a prime. Indeed, we already know that 641 is a prime divisor of F_5, and for the co-factor $c := \frac{F_5}{641} = 6\,700\,417$ we have $c - 1 = 2^7 \cdot 3 \cdot 17449$, and 5 turns out to be a Lucae primality witness.

Similarly, for $F_9 = 2^{64}+1$ we get $3^{\frac{F_9-1}{2}} \not\equiv -1 \pmod{F_9}$, implying that F_9 is not a prime. Indeed, we already know that $2\,424\,833$ is a prime divisor of F_9, and for the co-factor $c := \frac{F_9}{2424833}$ we get $3^{c-1} \not\equiv 1 \pmod{c}$, implying that c is not a prime, with Fermat decomposability witness 3. ♯

Finally, recall that for $n \in \mathbb{N}_0$ and $a := 2$ we have $2^{2^n} \equiv -1 \pmod{F_n}$, hence $2^{2^{n+1}} \equiv 1 \pmod{F_n}$, showing that $\overline{2} \in (\mathbb{Z}/F_n\mathbb{Z})^*$ has order 2^{n+1}. Since $2^{n+1} \mid 2^{2^n} = F_n - 1$, with equality if and only if $n \leq 1$, we conclude that 2 is a Lucas primality witness for F_0 and F_1, while it is a Fermat liar if F_n is decomposable, and does not yield any insights if F_n is a prime for $n \geq 2$.

V

15 References

[1] P. Bundschuh: Einführung in die Zahlentheorie, 6. Auflage, Springer, 2008.

[2] G. Hardy, E. Wright: An introduction to the theory of numbers, 5th edition, Oxford University Press, 1979.

[3] A. Schmidt: Einführung in die algebraische Zahlentheorie, Springer, 2007.

[4] R. Schulze-Pillot: Einführung in Algebra und Zahlentheorie, 3. Auflage, Springer, 2014.

[5] I. Stewart, D. Tall: Algebraic number theory, Chapman and Hall, 1987.

[6] J. von zur Gathen, J. Gerhard: Modern computer algebra, 2nd edition, Cambridge University Press, 2003.