3. Residue Class Rings

In this chapter we will study the conic $\mathcal{H} : XY = 1$ over residue class rings $\mathbb{Z}/m\mathbb{Z}$. The next step will be generalizing these results to general conics. For doing so, we will need some more abstract algebra (finite fields, in particular, which are the topic of the next chapter).

3.1. Fermat's First Theorem

Where we study the group law on the hyperbola over residue class rings.

Our main interest in this chapter lies with understanding the unit groups of the residue class rings $R = \mathbb{Z}/m\mathbb{Z}$. The material presented here is classical (going back to Gauss), and it is presented in the classical language. Later we will prove the results given here for a second time; in fact the properties of $(\mathbb{Z}/m\mathbb{Z})^\times \simeq \mathcal{H}(\mathbb{Z}/m\mathbb{Z})$ are shared by general conics.

We start by looking at the example of $\mathbb{Z}/5\mathbb{Z}$; the multiplication table for the nonzero elements in $\mathbb{Z}/5\mathbb{Z}$ is given by

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

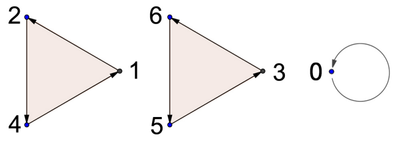
Such multiplication tables contain the full information about a group and its structure, but the structure is not visible. What we can see is the following:

- Every element has a multiplicative inverse because in every row and every column there is a 1;
- The group (if it is one) is abelian: commutativity is displayed by the fact that the table is symmetric with respect to the main diagonal.
- Elements of order 2 (here the residue classes generated by 1 and 4) can be found quickly: all we have to do is look for entries 1 on the diagonal.

On the other hand, checking associativity using the multiplication table is a horrible task. Similarly, such tables do not display subgroups.

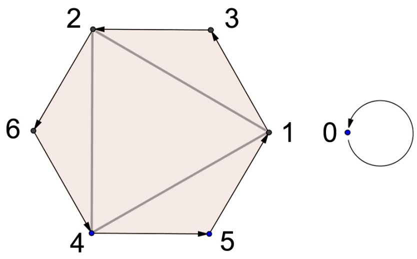
Multiplication in residue class rings $\mathbb{Z}/m\mathbb{Z}$ may be represented by a graph; multiplication by 2 in the ring $\mathbb{Z}/7\mathbb{Z}$, for example, is displayed as follows:

Multiplication by 2 produces a fixed point 0 (of course 0 is a fixed point for multiplication by any element) and two cycles of length 3. The cycle containing 1 forms a subgroup H of order 3 of the group G of nonzero elements modulo 7, the other cycle represents its coset G/H.



The picture for multiplication by 3 modulo 7 looks different:

Multiplication by 3 produces, except for the fixed point 0, a single cycle of length 6. In particular, every nonzero element of $\mathbb{Z}/7\mathbb{Z}$ can be written as a power of 3. The subgroup $\{[1],[2],[4]\}$ of the multiplicative group of nonzero elements in $\mathbb{Z}/7\mathbb{Z}$ is visible as a triangle inside the hexagon.
The complementary triangle represents the coset of G/H represented by [3].



Finally it is easily checked that multiplication by [6] produces three cycles of length 2.

It is no accident that the cycles for multiplication inside the group of nonzero elements modulo 7 have lengths 1, 2, 3 or 6: the fact that these cycle lengths divide $6 = 7 - 1$ generalizes to arbitrary prime numbers since Fermat's First Theorem will say that the cycle lengths for multiplication by nonzero elements modulo prime numbers p always divides $p - 1$.

In this section we will study the unit group $\mathcal{H}(\mathbb{Z}/p\mathbb{Z})$ for primes p, where $\mathcal{H} : XY = 1$ is a hyperbola. After an interlude on Fermat's Theorem on Sums of Two Squares we will study the group $\mathcal{H}(\mathbb{Z}/m\mathbb{Z}) \simeq (\mathbb{Z}/m\mathbb{Z})^\times$.

Fermat and Perfect Numbers

The Pythagoreans already studied perfect and amicable numbers. In our days, this area of mathematics is regarded as recreational mathematics. We will see, however, that Fermat came across ideas that are of central importance while studying perfect and amicable numbers.

Recall that a number n is called **perfect** if $\sigma(n) = 2n$, where $\sigma(n) = \sum_{d|n} 1$ is the sum of all divisors of n. Euclid only accepted proper divisors, so for him a number was perfect if it equaled the sum of its proper divisors. The two smallest perfect numbers are $6 = 2 \cdot 3$ and $28 = 4 \cdot 7$. Already Euclid knew the following

Fact 3.1. *If $M_p = 2^p - 1$ is a prime number, then $N = 2^{p-1}(2^p - 1)$ is perfect.*

The simple proof consists in verifying that the sum of the proper divisors $1 + 2 + 4 + \ldots + 2^{p-1} + M_p + 2M_p + \ldots + 2^{p-2}M_p$ equals N. Observe that for writing down the list of factors requires a special case of unique factorization for numbers of the form $2^n \cdot p$, where p is a prime number. Euclid, as well as many mathematicians afterwards, proved these special cases of unique factorization; the general observation that the factors of a number can be read off its prime factorization was occasionally stated, but the result was not seen as a basic and fundamental result in number theory before Gauss.

The only known primality test at the time of Fermat was finding prime factors; thus Fermat made tables of factors of number of the form $2^n - 1$ such as the following:

n	$2^n - 1$	n	$2^n - 1$	n	$2^n - 1$
2	3	6	$63 = 3^2 \cdot 7$	10	$1023 = 3 \cdot 11 \cdot 31$
3	7	7	127	11	$2947 = 23 \cdot 89$
4	$15 = 3 \cdot 5$	8	$255 = 3 \cdot 5 \cdot 17$	12	$4095 = 3^2 \cdot 5 \cdot 7 \cdot 13$
5	31	9	$511 = 7 \cdot 73$	13	8191

It is quickly seen that $2^m - 1 \mid 2^{mn} - 1$ for integers $n \geq 1$: this is an immediate consequence of the identity

$$x^{mn} - 1 = (x^m - 1)(x^{(m-1)n} + x^{(m-2)n} + \ldots + x^{2n} + x^n + 1).$$

Thus $2^n - 1$ is never prime if n is composite, and the only possible primes of the form $2^n - 1$ are the numbers $2^p - 1$ for primes p.

Lemma 3.2. *If $M_p = 2^p - 1$ is prime, then so is the exponent p.*

We will see below that the converse of this result is false.

Fermat noticed something else:

$$3 \mid 2^2 - 1, \quad 5 \mid 2^4 - 1, \quad 7 \mid 2^6 - 1, \quad 11 \mid 2^{10} - 1, \ldots$$

On the other hand, $9 \nmid 2^9 - 1$. This suggests the conjecture that if p is a prime number, then $p \mid 2^{p-1} - 1$.

Theorem 3.3 (Fermat's First Theorem)**.** *If p is a prime and a an integer not divisible by p, then $a^{p-1} \equiv 1 \bmod p$.*

There are various proofs for Fermat's First[1] Theorem. Here we will present a proof of Fermat's First theorem due to Euler that works for any finite group (for other proofs see the Exercises). To see what's going on, consider $(\mathbb{Z}/5\mathbb{Z})^\times = \{[1],[2],[3],[4]\}$, where $[r]$ denotes the residue class r mod 5. If we multiply each of these classes by 3, we get

$$\begin{aligned} [1] \cdot [3] &= [3], \\ [2] \cdot [3] &= [1], \\ [3] \cdot [3] &= [4], \\ [4] \cdot [3] &= [2]; \end{aligned}$$

thus multiplying all prime residue classes mod 5 by 3 yields the same classes again, though in a different order. If we multiply these four equations together, we get $[1][2][3][4] \cdot [3]^4 = [3][1][4][2] = [1][2][3][4]$, hence $[3]^4 = [1]$, or, in other words, $3^4 \equiv 1 \bmod 5$. This can be done in general:

Proof of Thm. 3.3. Write $(\mathbb{Z}/p\mathbb{Z})^\times = \{[1],[2],\ldots,[p-1]\}$; let a be an integer not divisible by p. If we multiply each residue class with $[a]$, the resulting residue classes are

$$\begin{aligned} [1] \cdot [a] &= [a] \\ [2] \cdot [a] &= [2a] \\ &\vdots \\ [p-1] \cdot [a] &= [(p-1)a] \end{aligned}$$

If we can show that the classes on the right hand side are all different, then they must be a permutation of the classes $[1]$, ..., $[p-1]$ that we started with. Taking this for granted, the products $[a] \cdot [2a] \cdots [(p-1)a] = [(p-1)!][a^{p-1}]$ and $[1] \cdot [2] \cdots [p-1] = [(p-1)!]$ must be equal (after all, the factors are just rearranged). But $(p-1)!$ is coprime to p, so we may cancel this factor, and get $[a^{p-1}] = [1]$, i.e., $a^{p-1} \equiv 1 \bmod p$.

It remains to show that the classes $[a]$, $[2a]$, ..., $[(p-1)a]$ are pairwise distinct. Assume therefore that $[ra] = [sa]$ for integers $1 \le r, s \le p-1$; we have to show that $r = s$. But $[ra] = [sa]$ means that $[(r-s)a] = [0]$, i.e. that $p \mid (r-s)a$. Since $p \nmid a$ by assumption, the fact that p is prime implies $p \mid (r-s)$. But $r - s$ is an integer strictly between $-p$ and p, and the only such integer divisible by p is 0: thus $r = s$ as claimed. □

[1] In the literature, this result is usually called Fermat's Little Theorem in contrast to Fermat's Great Theorem, the unsolvability of $x^n + y^n = z^n$ in positive integers for exponents $n > 2$. This last result is nowadays called Fermat's Last Theorem and was proved by A. Wiles.

The **order** of an element of a group G is the smallest positive integer n such that $g^n = 1$. If g has order n, then the subgroup $H = \langle g \rangle$ generated by g has order n, and Prop. 2.3 tells us that $n \mid \#G$. Applied to the group $G = (\mathbb{Z}/p\mathbb{Z})^\times$ with order $p-1$, this means that $a^{p-1} \equiv 1 \bmod p$ for every integer a coprime to p. This proof also explains our observation made at the beginning of this chapter that the cycle length of an element $a \in \mathbb{Z}/(p\mathbb{Z})^\times$ (this coincides with the order of a) always divides $p-1$.

Fermat's First Theorem can be expressed in the language of conics as follows: let $\mathcal{H} : XY = 1$ denote the hyperbola, let p denote a prime number, and consider a point $P = (a, a^{-1}) \in \mathcal{H}(\mathbb{Z}/p\mathbb{Z})$. Then $(p-1) \cdot P = N$, where $N = (1, 0)$ is the neutral element in $\mathcal{H}(\mathbb{Z}/p\mathbb{Z})$. This form of Fermat's First Theorem generalizes to arbitrary Pell conics.

We finally remark that Fermat's First Theorem also may be used for computing the multiplicative inverse of a mod p. In fact, we can simply set $a^{-1} \equiv a^{p-2} \bmod p$. Computing $a^{p-2} \bmod p$ may seem to require a lot more time than using the Euclidean algorithm for computing the inverse of $a \bmod p$ via the Bezout relation; we will see in Chap. 5, however, that there are fast methods of exponentiation that allow us to computate $a^{-1} \equiv a^{p-2} \bmod p$ rather quickly.

3.2. The Legendre Symbol

Where we study the quadratic character of small integers.

We start by observing the following facts concerning the group structures on the parabola $\mathcal{P} : Y = X^2$ and the hyperbola $\mathcal{H} : XY = 1$. We start by fixing an arbitrary field K. In the case of the parabola, the map $K \longrightarrow \mathcal{P}(K) : t \to (t, t^2)$ provides us, on the one hand, with a rational parametrization of the parabola: every point in $\mathcal{P}(K)$ has the form (t, t^2) with $t \in K$. On the other hand, this parametrization also is a group homomorphism that tells us that the group of K-rational points on the parabola is isomorphic to the additive group of the field K.

In the case of the hyperbola, we similarly have a map $K^\times = K \setminus \{0\} \longrightarrow \mathcal{H}(K) : t \to (t, \frac{1}{t})$, which is, on the one hand, a rational parametrization of the hyperbola: every K-rational point on $\mathcal{H}$ has the form $(t, \frac{1}{t})$ for some nonzero $t \in K$. On the other hand, this parametrization again gives us a group isomorphism $K^\times \simeq \mathcal{H}(K)$.

Now consider the unit circle $\mathcal{C} : X^2 + Y^2 = 1$. We have found a parametrization of its K-rational points in (1.4): the map

$$t \to \Big(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\Big)$$

sends an element $t \in K$ to a K-rational point on the unit circle, but this time there are three problems:

1. The point $(-1, 0)$ on the unit circle is not among the parametrized points.
2. The parametrization only gives points with vanishing y-coordinates when K has characteristic 2; in this case, the unit circle is a union of two identical lines since $X^2 + Y^2 - 1 = (X + Y + 1)^2$.
3. The parametrization is not defined for all $t \in K$ since the denominator $t^2 + 1$ might vanish.

The last item is particularly interesting for fields $K = \mathbb{Z}/p\mathbb{Z}$. For $p = 3$, the polynomial $T^2 + 1$ does not have a root, for $p = 5$ there are two of them, namely $t = 2$ and $t = 3$. For odd primes p we define the **Legendre symbol**

$$\Big(\frac{-1}{p}\Big) = \begin{cases} -1 & \text{if } t^2 \equiv -1 \bmod p \text{ has no solution,} \\ +1 & \text{if } t^2 \equiv -1 \bmod p \text{ has a solution.} \end{cases}$$

Our two examples have shown that $(\frac{-1}{3}) = -1$ and $(\frac{-1}{5}) = +1$.

The parametrization (1.4) of the unit circle over $K = \mathbb{Z}/p\mathbb{Z}$ gives every point $\ne (-1,0)$ on $\mathcal{C}(K)$, and is defined for all $t \in K$ except the at most two values of t for which $t^2+1 = 0$ in K. The right hand side of (1.4) is defined for all $t \in K$ except for $1 + (\frac{-1}{p})$ values of t, hence the parametrization gives us $p - 1 - (\frac{-1}{p})$ different points on $\mathcal{C}(K)$. Since $(-1,0)$ is not among them, we have found $p - (\frac{-1}{p})$ points in $\mathcal{C}(K)$, and the usual geometric argument[2] shows that these are all K-rational points. Thus we have proved

Proposition 3.4. *Let $\mathcal{C} : X^2 + Y^2 = 1$ be the unit circle defined over $\mathbb{Z}/p\mathbb{Z}$ for an odd prime number p. The number of points on $\mathcal{C}(\mathbb{Z}/p\mathbb{Z})$ is given by*

$$\#\mathcal{C}(\mathbb{Z}/p\mathbb{Z}) = p - \Big(\frac{-1}{p}\Big) = \begin{cases} p-1 & \textit{if } t^2 \equiv -1 \bmod p \textit{ is solvable}, \\ p+1 & \textit{if } t^2 \equiv -1 \bmod p \textit{ is not solvable.} \end{cases}$$

Of course we would like to know for which primes p the congruence $t^2 \equiv -1 \bmod p$ has a solution. This problem is called the determination of the quadratic character of -1 modulo p, and is one out of many challenging similar problems that we will come across over and over again in this book before we will give a definite anwser to such problems in Chap. 7 on the modularity of Pell conics.

For finding the quadratic character of -1, the group structure on the unit circle comes to our rescue. Observe that the point $P = (0,1)$ lies in $\mathcal{C}(\mathbb{Z}/p\mathbb{Z})$ for every prime number p, and that $2P = (-1,0)$ and $4P = (1,0) = N$. This shows that P has order 4 on $\mathcal{C}(\mathbb{Z}/p\mathbb{Z})$, hence $\#\mathcal{C}(\mathbb{Z}/p\mathbb{Z})$ must be a multiple of 4 by Prop. 2.3. Since the group order is $p \pm 1$, we must have

$$\mathcal{C}(\mathbb{Z}/p\mathbb{Z}) = \begin{cases} p-1 & \text{if } p \equiv 1 \bmod 4, \\ p+1 & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

Comparing this with the result from Prop. 3.4 we find

Proposition 3.5. *For odd prime numbers p we have*

$$\Big(\frac{-1}{p}\Big) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1 & \textit{if } p \equiv 1 \bmod 4, \\ -1 & \textit{if } p \equiv 3 \bmod 4. \end{cases}$$

In particular, the congruence $x^2 \equiv -1 \bmod p$ is solvable if and only if $p \equiv 1 \bmod 4$.

This result is far from being a trivial observation. It is the basis of Fermat's Two-Squares Theorem, and will appear later on in the disguise of the modularity of the unit circle. Although we could prove the Two-Squares Theorem with the methods we have provided so far, we will postpone the proof to the next section.

In addition, it gives us the following result:

Proposition 3.6. *There exist infinitely many prime numbers of the form $p \equiv 3 \bmod 4$, and infinitely many of the form $p \equiv 1 \bmod 4$.*

For proving the first claim, assume that we know primes $p_1, \ldots, p_n$ of the form $p_j \equiv 3 \bmod 4$, and consider $N = 4p_1 \cdots p_n - 1$. Since $N \equiv 3 \bmod 4$, all of its prime divisors are odd, and not all of them can be $\equiv 1 \bmod 4$ (otherwise we would have $N \equiv 1 \bmod 4$). Since $N > 1$ there is at least one prime $p \equiv 3 \bmod 4$ dividing N, and if we had $p = p_j$, then p would divide both N and $N + 1 = 4p_1 \cdots p_n$, which is impossible. Thus we have found a new prime $p \equiv 3 \bmod 4$, which shows that their number cannot be finite.

[2] Take any K-rational point $(x,y) \ne (-1,0)$; the slope $t = \frac{y}{x+1}$ gives the value for which (x,y) shows up in the parametrization.

The proof for primes $p \equiv 1 \bmod 4$ requires a different method (why does looking at $N = 4p_1 \cdots p_n + 1$ not work?). Assume that we have primes $p_1, \ldots, p_n$ of the form $p_j \equiv 1 \bmod 4$, and consider the number $N = (2p_1 \cdots p_n)^2 + 1$. This is an odd integer and a sum of two coprime squares; the following lemma shows that all of its prime divisors have the form $p \equiv 1 \bmod 4$. Since $p = p_j$ would imply that p divides both N and $N - 1$, this prime p is not in our list, and again the number of primes $p \equiv 1 \bmod 4$ cannot be finite.

Here is the missing lemma:

Lemma 3.7. *If $N = x^2 + y^2$ for coprime integers x, y, then $p \mid N$ implies $p = 2$ or $p \equiv 1 \bmod 4$.*

Proof. Assume that $p \mid N$. Then $x^2 \equiv -y^2 \bmod p$; if we had $p \mid y$, then $p \mid x$ as well, contradicting the assumption that x and y are coprime. Thus $p \nmid y$, hence $-1 \equiv (x/^y)^2 \bmod p$ is congruent to a square modulo p. By our results above, this can only happen if $p = 2$ or $p \equiv 1 \bmod 4$. □

For general numerators, the **Legendre symbol** $(\frac{a}{p})$ is defined for all odd primes p and all integers a by setting

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{if } x^2 \equiv a \bmod p \text{ for some } a \in (\mathbb{Z}/p\mathbb{Z})^\times, \\ 0 & \text{if } p \mid a, \\ -1 & \text{otherwise.} \end{cases}$$

An integer a coprime to the odd prime p is called a **quadratic residue** modulo p if $(\frac{a}{p}) = +1$, and a **quadratic nonresidue** otherwise.

Fact 3.8. *If r, r' are quadratic residues modulo p and n a quadratic nonresidue, then rr' is a quadratic residue, and nr a quadratic nonresidue modulo p.*

It is also true that if n and n' are quadratic nonresidues, then nn' is a quadratic residue. This property is less trivial than those mentioned above and will follow from our results below. The fact that the last property lies deeper can also be seen from the observation that the first two claims hold in every field: if r, r' are squares and if n is a nonsquare in some field R, then clearly rr' is a square, and rn is a nonsquare in R. If, however, n and n' are nonsquares, then it does not follow in general that nn' is a square: there is a wealth of counterexamples even in the field of rational numbers, where 2, 3 and their product 6 are nonsquares. The different behaviour of the fields $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Q}$ in this respect is a reflection of the fact to be proved later that there is a unique quadratic extension (unique up to isomorphism, to be more precise) of $\mathbb{Z}/p\mathbb{Z}$, namely the field with p^2 elements, whereas $\mathbb{Q}$ admits infinitely many distinct quadratic extensions. An equivalent formulation is that $U = (\mathbb{Z}/p\mathbb{Z})^\times$ has a finite quotient $U/U^2 \simeq \mathbb{Z}/2\mathbb{Z}$, whereas $\mathbb{Q}^\times/\mathbb{Q}^{\times\,2}$ is a really big group, consising of infinitely many copies of $\mathbb{Z}/2\mathbb{Z}$.

The most fundamental properties of the Legendre symbol are the following:

Fact 3.9. *Let p be an odd prime number. Among the $p - 1$ residue classes coprime to p there are $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic nonresidues.*

There is another characterization of the Legendre symbol $(\frac{a}{p})$ due to Euler:

Proposition 3.10 (Euler's criterion)**.** *For odd prime numbers p and integers a not divisible by p we have*

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \mod p.$$

Our proof goes back to Euler himself: let $p = 2m+1$ be prime. If $a \equiv b^2 \bmod p$ is a square, then $a^{(p-1)/2} \equiv b^{p-1} \equiv 1 \bmod p$ by Fermat's First Theorem. Conversely, assume that $a^k \equiv 1 \bmod p$ for $k = \frac{p-1}{2}$, and let $a_1, \ldots, a_k$ denote the quadratic residues modulo p. If a is a quadratic nonresidue modulo p, then $a_1a, \ldots, a_ka$ are quadratic nonresidues (and in fact all k of them). But then $x^k \equiv 1 \bmod p$ for all the quadratic residues $x = a_i$ and all the nonresidues $x = a_ia$ as well since $(a_ia)^k \equiv a^k \equiv 1 \bmod p$. Since the polynomial $X^k - 1$ has at most m roots in the finite field $\mathbb{Z}/p\mathbb{Z}$, this is impossible.

Euler's criterion immediately implies that Legendre symbols are multiplicative in the numerator:

Corollary 3.11. *For all odd primes p and all integers a, b not divisible by p we have*

$$\Big(\frac{a}{p}\Big)\Big(\frac{b}{p}\Big) = \Big(\frac{ab}{p}\Big).$$

This implies in particular that $a + p\mathbb{Z} \mapsto (\frac{a}{p})$ is a group homomorphism

$$(\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow \mu_2 = \{-1, +1\}.$$

Since $(\mathbb{Z}/p\mathbb{Z})^\times = \langle g \rangle$ is cyclic, there is in fact a unique nontrivial homomorphism $(\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow \mu_2$, which necessarily must coincide with the map induced by the Legendre symbol.

We can use this property to generalize the Legendre symbol to composite integers by defining a homomorphism $(\mathbb{Z}/m\mathbb{Z})^\times \longrightarrow \mu_2$ that is compatible with the Chinese Remainder Theorem: if $n = p_1 \cdots p_r$ is a product of (not necessarily distinct) primes p_j, then we set

$$\Big(\frac{a}{n}\Big) = \Big(\frac{a}{p_1}\Big) \cdots \Big(\frac{a}{p_r}\Big).$$

This symbol $(\frac{a}{n})$ is called the **Jacobi symbol**. For prime values of n, it coincides with the Legendre symbol. Observe, however, that $(\frac{a}{n}) = +1$ does not imply that a is a square modulo n; we have, for example, $(\frac{2}{15}) = (\frac{2}{3})(\frac{2}{5}) = (-1) \cdot (-1) = +1$, yet 2 is not a square modulo 15 since it is not even a square modulo 3.

In Prop. 3.4 we have shown that

$$\Big(\frac{-1}{p}\Big) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1 & \text{if } p \equiv 1 \bmod 4, \\ -1 & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

This may now bw generalized to aribtrary positive odd integers n: we have

$$\Big(\frac{-1}{n}\Big) = (-1)^{\frac{n-1}{2}} = \begin{cases} +1 & \text{if } n \equiv 1 \bmod 4, \\ -1 & \text{if } n \equiv 3 \bmod 4. \end{cases}$$

In fact assume that $n = p_1 \cdots p_n$. If an even number of p_j satisfy $p_j \equiv -1 \bmod 4$, then $n \equiv 1 \bmod 4$, and we have $\prod_j (\frac{-1}{p_j}) = 1$. If an odd number of p_j satisfy $p_j \equiv -1 \bmod 4$, then $n \equiv 3 \bmod 4$, and we have $\prod_j (\frac{-1}{p_j}) = -1$.

Determining Legendre symbols $(\frac{a}{p})$ for other values of a in terms of simple criteria for p is difficult. In the following we will use the group structure on Pell conics to determine the quadratic character of ± 2 and ± 3. For larger integers a, giving similar characterizations of $(\frac{a}{p})$ is a challenging problem, which we will meet again in the guise of "modularity" of Pell conics, in particular in Chap. 7 below.

For determining the Legendre symbol $(\frac{2}{p})$ we will use the conic $\mathcal{C}_2 : X^2 + Y^2 = 2$. Given a point $P = (x, y) \in \mathcal{C}(\mathbb{Z}/p\mathbb{Z})$, the points in the set

$$S_P = \{(\pm x, \pm y), (\pm y, \pm x)\}$$

also lie on $\mathcal{C}(\mathbb{Z}/p\mathbb{Z})$. These sets S_P contain 8 elements except in the following cases:

1. S_P only contains 4 elements if $P = (\pm 1, \pm 1)$.
2. If $(\frac{2}{p}) = 1$, then $x^2 = 2$ for some $x \in \mathbb{F}_p$, and the point $Q = (x, 0)$ generates $S_Q = \{(\pm x, 0), (0, \pm x)\}$, which again has 4 elements.

This implies that $\#\mathcal{C}_2(\mathbb{F}_p) \equiv 0 \bmod 8$ if Q exists, and that $\#\mathcal{C}_2(\mathbb{F}_p) \equiv 4 \bmod 8$ otherwise.

On the other hand, the substitutions $X = U + V$, $Y = U - V$ transform $X^2 + Y^2 = 2$ into the unit circle $U^2 + V^2 = 1$, and the inverse map $U = \frac{1}{2}(X+Y)$, $V = \frac{1}{2}(X-Y)$ shows that this transformation is a bijection on $\mathcal{C}_2(\mathbb{F}_p)$ for odd primes p. Thus $\mathcal{C}_2(\mathbb{F}_p) = p - (\frac{-1}{p})$.

The fact that $\#\mathcal{C}_2(\mathbb{F}_p)$ is divisible by 4 gives a new proof of Prop. 3.4. We now distinguish the following cases:

1. $p \equiv 1 \bmod 8$. Then $\#\mathcal{C}_2(\mathbb{F}_p) = p - 1 \equiv 0 \bmod 8$, hence $(\frac{2}{p}) = +1$.
2. $p \equiv 3 \bmod 8$. Then $\#\mathcal{C}_2(\mathbb{F}_p) = p + 1 \equiv 4 \bmod 8$, hence $(\frac{2}{p}) = -1$.
3. $p \equiv 5 \bmod 8$. Then $\#\mathcal{C}_2(\mathbb{F}_p) = p - 1 \equiv 4 \bmod 8$, hence $(\frac{2}{p}) = -1$.
4. $p \equiv 7 \bmod 8$. Then $\#\mathcal{C}_2(\mathbb{F}_p) = p + 1 \equiv 0 \bmod 8$, hence $(\frac{2}{p}) = +1$.

We have proved

Proposition 3.12. *For odd primes p we have*

$$\Big(\frac{2}{p}\Big) = \begin{cases} +1 & \textit{if } p \equiv \pm 1 \bmod 8, \\ -1 & \textit{if } p \equiv \pm 3 \bmod 8. \end{cases}$$

Exactly as in the case of $(\frac{-1}{p})$, this result may be used for proving the existence of infinitely many primes with prescribed character $(\frac{2}{p})$:

Proposition 3.13. *There exist infinitely many primes p with $(\frac{2}{p}) = -1$, and infinitely many with $(\frac{2}{p}) = +1$.*

The results concerning the quadratic characters of -1 and 2 may be combined to yield the quadratic character of -2: the multiplicativity of the Legendre symbol tells us that $(\frac{-2}{p}) = (\frac{-1}{p})(\frac{2}{p})$; this implies

Corollary 3.14. *For odd primes p we have*

$$\Big(\frac{-2}{p}\Big) = \begin{cases} +1 & \textit{if } p \equiv 1, 3 \bmod 8, \\ -1 & \textit{if } p \equiv 5, 7 \bmod 8. \end{cases}$$

If $p \equiv 3 \bmod 8$, for example, we have $(\frac{-1}{p}) = -1$ and $(\frac{2}{p}) = +1$, hence $(\frac{-2}{p}) = (\frac{-1}{p})(\frac{2}{p}) = -1$ as claimed. The other cases follow in a similar way.

Our result on the quadratic character of 2 has a number of interesting corollaries. One of them concerns the prime divisors of Mersenne numbers $M_p = 2^p - 1$. We have already seen that if $q \mid M_p$ for prime numbers p, then $q \equiv 1 \bmod p$. Now we can improve this:

Corollary 3.15. *Let p be an odd prime number, and let q be a prime dividing $M_p = 2^p - 1$. Then $q \equiv \pm 1 \bmod 8$.*

This follows easily from the observation that if $p = 2m + 1$, then $2^p \equiv 1 \bmod q$ implies $2 \cdot (2^m)^2 \equiv 1 \bmod q$, and this shows that 2 is a square mod q.

Now we will investigate $(\frac{-3}{p})$.

Proposition 3.16. *For prime numbers $p \neq 3$ we have*

$$\Big(\frac{-3}{p}\Big) = \begin{cases} +1 & \textit{if } p \equiv 1 \bmod 3, \\ -1 & \textit{if } p \equiv 2 \bmod 3. \end{cases}$$

We prove this result by looking at the "Eisenstein conic" $\mathcal{C} : X^2 + XY + Y^2 = 1$. We have $\varphi_{\mathcal{C}}(p) = p - (\frac{-3}{p})$. On the other hand, the map $\rho : (x, y) \mapsto (-y, x - y)$ satisfies $\rho^2((x, y)) = \rho((-y, x - y)) = (y - x, -x)$ and $\rho^3((x, y)) = \rho((y - x, -x)) = (x, y)$. Thus the points on $\mathcal{C}(\mathbb{Z}/p\mathbb{Z})$ come in groups of three, except for the points fixed by ρ. Now $\rho((x, y)) = (x, y)$ if and only if $x = -y$ and $y = x - y$, which implies $x = y = 0$. Since this is impossible, $\phi_{\mathcal{C}}(p)$ must be a multiple of 3. This implies $(\frac{-3}{p}) \equiv p \bmod 3$, which in turn implies the claim.

The multiplicativity of the Kronecker symbol shows that $(\frac{3}{p}) = (\frac{-1}{p})(\frac{-3}{p})$, which gives us, in a similar way as above, the following

Corollary 3.17. *For all primes $p > 3$ we have*

$$\Big(\frac{3}{p}\Big) = \begin{cases} +1 & \text{if } p \equiv \pm 1 \bmod 12, \\ -1 & \text{if } p \equiv \pm 5 \bmod 12. \end{cases}$$

3.3. Sums of Two Squares

Where we prove a beautiful theorem by Fermat.

Which numbers can be written as sums of two squares? This is one out of a gazillion of similar questions, such as

- Which numbers can be written as sums of two primes?
- Which numbers can be written as a sum of a prime number and a square?

What makes the problem of two squares interesting is the fact that there is a beautiful answer, and that there are connections with higher arithmetic (quadratic number fields) or even complex analysis (theta functions).

Here is a short table of representations of positive integers n as sums $a^2 + b^2$ of two squares:

n	1	2	3	4	5	6	7	8	9	10	11	12	13
(a, b)	$(1, 0)$	$(1, 1)$	$-$	$(2, 0)$	$(1, 2)$	$-$	$-$	$(2, 2)$	$(3, 0)$	$(1, 3)$	$-$	$-$	$(3, 2)$

We can see that the primes $p = 2$, 5, 13 are sums of two squares, and that 3, 7, and 11 are not. The last observation can be explained easily by the following observation:

Proposition 3.18. *If a prime p is the sum of two integral squares, then $p = 2$ or $p \equiv 1 \bmod 4$.*

Proof. There are four residue classes modulo 4; their squares are $[0] = [0]^2 = [2]^2$ and $[1] = [1]^2 = [3]^2$.

Now assume that $p = a^2 + b^2$. Since $a^2, b^2 \equiv 0, 1 \bmod 4$, we find that $a^2 + b^2$ must be congruent modulo 4 to one of $0 = 0 + 0$, $1 = 1 + 0 = 0 + 1$, or $2 = 1 + 1$, that is, $p \equiv 0, 1, 2 \bmod 4$. Since no prime is congruent to $0 \bmod 4$, and since 2 is the only prime $\equiv 2 \bmod 4$, we even have $p = 2$ or $p \equiv 1 \bmod 4$ as claimed. □

Already Fermat could prove that Prop. 3.18 can be sharpened considerably:

Proposition 3.19. *If q is an odd prime dividing a sum of two coprime integral squares, then $q \equiv 1 \bmod 4$.*

Proof. Our first proof goes like this: if $q \mid (x^2+y^2)$, then $x^2+y^2 \equiv 0 \bmod q$, hence $x^2 \equiv -y^2 \bmod q$. Raising both sides to the $\frac{q-1}{2}$-th power we find $1 \equiv (-1)^{(q-1)/2} \bmod q$, where we have used that $q \nmid y$: otherwise we also have $q \mid x$, contradicting our assumption that x and y are coprime.

Here's a different proof, which is perhaps close to Fermat's own proof. Assume that $q \mid a^2+b^2$ for coprime integers a and b. If a and b are both odd, then $c = \frac{a+b}{2}$ and $d = \frac{a-b}{2}$ are integers with different parity since $c+d=a$ is odd. The identity $a^2+b^2 = 2(c^2+d^2)$ now shows that q also divides a sum of two coprime squares with different parity.

Thus we may write $qm = a^2+b^2$ for some odd integer m. Replacing a and b by their minimal remainders modulo q we may assume that a and b are both less than $\frac12 q$. Thus $a^2+b^2 < \frac12 q^2$, and this implies $m < \frac12 q$. This shows that $m < q$ divides a sum of two coprime squares, and if $q \equiv 3 \bmod 4$, then the fact that $qm = a^2+b^2 \equiv 1 \bmod 4$ implies that $m \equiv 3 \bmod 4$. In particular, m has a prime factor $q_1 \equiv 3 \bmod 4$, and this q_1 divides a sum of two coprime squares.

Thus if a prime number $q \equiv 3 \bmod 4$ divides a sum of two coprime squares, then there is a prime $q_1 < q$ with the same properties. But this is impossible. □

For the converse, we need to know when $[-1]$ is a square in $\mathbb{Z}/p\mathbb{Z}$ for primes p. Experiments show that $[-1]$ is not a square modulo 3, 7, or 11, and that $[2]^2 = [-1]$ for $p=5$, and $[5]^2 = [-1]$ for $p = 13$. The general result is

Proposition 3.20. *For odd prime numbers p, the the congruence $a^2 \equiv -1 \bmod p$ has a solution if and only if $p \equiv 1 \bmod 4$.*

Recall that we have already given a proof of this result in Prop. 3.5. One half of this proposition follows easily from Fermat's First Theorem: if $x^2 \equiv -1 \bmod p$ is solvable, then raising this congruence to the $\frac{p-1}{2}$-th power yields $x^{p-1} \equiv (-1)^{(p-1)/2} \bmod p$. Since the left hand side is $\equiv 1 \bmod p$ by Fermat's First Theorem, we conclude that $\frac{p-1}{2}$ must be even, and this means $p \equiv 1 \bmod 4$.

We will next give a constructive proof of the converse, that is, a proof not only showing that the congruence in question has a solution but a proof that actually exhibits such a solution. To this end, we use Wilson's Theorem (Prop. 2.9), according to which $(p-1)! \equiv -1 \bmod p$ for prime numbers p, for giving another proof of the solvability of $x^2 \equiv -1 \bmod p$ for prime numbers $p \equiv 1 \bmod 4$.

Proposition 3.21. *Put $a = (\frac{p-1}{2})!$, where p is an odd prime number p. Then*

$$a^2 \equiv (-1)^{(p+1)/2} \bmod p.$$

In particular, $a \equiv \pm 1 \bmod p$ if $p \equiv 3 \bmod 4$, and $a^2 \equiv -1 \bmod p$ if $p \equiv 1 \bmod 4$.

Proof. We start with Wilson's theorem $(p-1)! \equiv -1 \bmod p$; if, in the product $(p-1)!$, we replace the elements $\frac{p+1}{2}, \frac{p+3}{2}, \ldots, p-1$ by their negatives $-\frac{p+1}{2} \equiv \frac{p-1}{2}$, $-\frac{p+3}{2} \equiv \frac{p-3}{2}$, $\ldots$, $-(p-1) \equiv 1 \bmod p$, then we have introduced exactly $\frac{p-1}{2}$ factors -1; thus $-1 \equiv (p-1)! \equiv (-1)^{(p-1)/2} a^2 \bmod p$ with $a = (\frac{p-1}{2})!$). This proves the claim. □

Now we can prove Proposition 3.20: if $p \equiv 1 \bmod 4$, then we have just constructed a solution of the congruence $a^2 \equiv -1 \bmod p$. The converse is also true: if p is an odd prime such that $a^2 \equiv -1 \bmod p$ has a solution, then p must be $\equiv 1 \bmod 4$. This will follow from Fermat's Little Theorem.

The solvability of $x^2 \equiv -1 \bmod p$ is the first of two steps in our proof of the Theorem of Girard-Fermat; if x is such a solution, and if $x \equiv \frac{a}{b} \bmod p$ for coprime integers a, b, then $a \equiv bx \bmod p$, and squaring shows that $a^2 \equiv -b^2 \bmod p$, that is, p divides the sum of two coprime squares a^2+b^2. If we can make a and b small simultaneously, say $< \sqrt{p}$, then a^2+b^2 will be a multiple of p satisfying $0 < a^2+b^2 < 2p$, from which we will be able to conclude that $p = a^2+b^2$. Thus all we need is the following result due to Thue:

Proposition 3.22. *Given an integer a not divisible by p, there exist $x, y \in \mathbb{Z}$ with $0 < |x|, |y| < \sqrt{p}$ such that $ay \equiv x \bmod p$.*

Proof. Let f be the smallest integer greater than $\sqrt{p}$, and consider the residue classes $\{[u+av] : 0 \le u, v < f\}$ modulo p. There are $f^2 > p$ such expressions, but only p different residue classes, hence there must exist u, u', v, v' such that $u + av \equiv u' + av' \bmod p$. Put $x = u - u'$ and $y = v' - v$; then $x \equiv ay \bmod p$, and moreover $-f < x, y < f$. □

Now we can prove

Theorem 3.23 (Girard-Fermat-Euler). *Every prime $p \equiv 1 \bmod 4$ is a sum of two integral squares.*

Proof. Since $p \equiv 1 \bmod 4$, there is an $a \in \mathbb{Z}$ such that $a^2 \equiv -1 \bmod 4$. By Thue's result, there are integers x and y such that $ay \equiv x \bmod p$ and $0 < x, y < \sqrt{p}$. Squaring gives $-y^2 \equiv x^2 \bmod p$, that is, $x^2+y^2 \equiv 0 \bmod p$. Since $0 < x^2, y^2 < p$, we find $0 < x^2+y^2 < 2p$; since x^2+y^2 is divisible by p, we must have $x^2+y^2 = p$. □

This result can be extended to positive integers using Brahmagupta's identity

$$(a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2,$$

which bears a certain resemblance with the addition law on the unit circle (and this is, of course, not an accident). In fact it can be shown that a positive integer n is a sum of two squares if and only if every prime divisor $q \equiv 3 \bmod 4$ of n occurs in the prime factorization of n with even multiplicity.

In exactly the same way as the Two-Squares Theorem we now can prove

Corollary 3.24. *An odd prime number p is represented by the form X^2+2Y^2 if and only if $p \equiv 1, 3 \bmod 8$.*

Clearly $p = x^2+2y^2 \equiv 1, 3 \bmod 8$ according as y is odd or even. Assume conversely that $p \equiv 1, 3 \bmod 8$. Then $a^2 \equiv -2 \bmod p$ for some integer a. By Thue's Prop. 3.22 there exist integers x, y with $ay \equiv x \bmod p$ and $0 < x, y < \sqrt{p}$. Thus $0 < x^2+2y^2 < 3p$, where $x^2+2y^2 \equiv 0 \bmod p$. If $p = x^2+2y^2$, then we are done. If not, then $x^2+2y^2 = 2p$; but then $x = 2x_1$ is even, and we have $y^2+2x_1^2 = p$. This proves our claim.

In the same way we can prove

Corollary 3.25. *An odd prime number p is represented by the form X^2-2Y^2 if and only if $p \equiv \pm 1 \bmod 8$.*

Here you will have to observe that if $x^2-2y^2 = -p$, then $(x+2y)^2 - 2(x+y)^2 = +p$.

Exactly as above we now can use Thue's result for proving

Corollary 3.26. *An odd prime number p is represented by the form X^2+3Y^2 if and only if $p \equiv 1 \bmod 3$.*

In the proof you will have to use the fact that $x^2+3y^2 = 2p$ is impossible modulo 4, and that $x^2+3y^2 = 3p$ leads to $y^2+3x_1^2 = p$. The corresponding result for the form X^2-3Y^2 is

Corollary 3.27. *An odd prime number p is represented by the form X^2-3Y^2 if and only if $p \equiv 1 \bmod 12$; the prime $-p$ is represented by X^2-3Y^2 if and only if $p \equiv 11 \bmod 12$.*

Some of the analogous result for forms X^2-mY^2 with $|m| \ge 5$ can still be proved with the same elementary methods. A proper understanding of what is going on here requires methods from the theory of binary quadratic forms, which we intend to cover in a sequel to this book.

3.4. The Theorem of Euler-Fermat

Where we generalize Fermat's First Theorem to composite moduli.

We start by looking at the example of $\mathbb{Z}/6\mathbb{Z}$; the multiplication table for the nonzero elements in $\mathbb{Z}/6\mathbb{Z}$ is given by

	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

The multiplication table of $\mathbb{Z}/6\mathbb{Z}$ above shows that the residue classes generated by 2, 3 and 4 are zero divisors, and that the only units in $\mathbb{Z}/6\mathbb{Z}$ are the residue classes generated by 1 and 5. These are the only residue classes containing numbers coprime to 6, and this observation generalizes.

In fact we next will prove that the units in the ring $\mathbb{Z}/m\mathbb{Z}$ are the residue classes $[a]$ with $\gcd(a, m) = 1$. It is now that the Bezout representation begins to show its full power. In fact, if $\gcd(a, m) = 1$, then there exist integers $x, y \in \mathbb{Z}$ such that $ax + my = 1$. Reducing this equation modulo m gives $ax \equiv 1 \bmod m$, in other words: the residue class $a \bmod m$ is a unit! Not only that: the extended Euclidean algorithm gives us a method for computing the inverse elements.

To prove the converse, assume that $a \bmod m$ is a unit. Then $ac \equiv 1 \bmod m$ for some $c \in \mathbb{Z}$, so $ac = km + 1$ for some $k \in \mathbb{Z}$. But then $ac - km = 1$ shows that $\gcd(a, m) = 1$.

We have shown

Theorem 3.28. *We have* $(\mathbb{Z}/m\mathbb{Z})^\times = \{a \bmod m : \gcd(a, m) = 1\}$.

Now consider the unit group $(\mathbb{Z}/15\mathbb{Z})^\times$ of $\mathbb{Z}/15\mathbb{Z}$. It consists of the eight residue classes [1], [2], [4], [7], [8], [11], [13], [14]. If we multiply each of these classes e.g. by [7] (or [8], [9]), then we get

$$\begin{array}{rcl}
[1]\cdot[7] = [7] & [1]\cdot[8] = [8] & [1]\cdot[9] = [9] \\
[2]\cdot[7] = [14] & [2]\cdot[8] = [1] & [2]\cdot[9] = [3] \\
[4]\cdot[7] = [13] & [4]\cdot[8] = [2] & [4]\cdot[9] = [6] \\
[7]\cdot[7] = [4] & [7]\cdot[8] = [11] & [7]\cdot[9] = [3] \\
[8]\cdot[7] = [11] & [8]\cdot[8] = [4] & [8]\cdot[9] = [12] \\
[11]\cdot[7] = [2] & [11]\cdot[8] = [13] & [11]\cdot[9] = [9] \\
[13]\cdot[7] = [1] & [13]\cdot[8] = [14] & [13]\cdot[9] = [12] \\
[14]\cdot[7] = [8] & [14]\cdot[8] = [7] & [14]\cdot[9] = [6]
\end{array}$$

As in our proof of Fermat's First Theorem, the resulting residue classes (for multiplication by [7] and [8]) are the classes we started with in a different order. Multiplying these equations we get

$$\prod_{(a,15)=1} [a] = \prod_{(a,15)=1} [7a] = [7]^8 \prod_{(a,15)=1} [a].$$

Since the a are coprime to 15, so is their product; thus we may cancel $\prod[a]$, and we find $[7]^8 = [1]$, or $7^8 \equiv 1 \bmod 15$. Similarly, we find $8^8 \equiv 1 \bmod 15$; for multiplication by 9, however, the classes on the right hand side differ from those on the left (they're all divisible by 3 since both 9 and 15 are), and we do *not* get $9^8 \equiv 1 \bmod 15$.

The same idea works in general. Let $m \ge 2$ be an integer, and let $\varphi(m)$ denote the number of residue classes coprime to m, that is, $\varphi(m) = \#(\mathbb{Z}/m\mathbb{Z})^\times$. Then we have the following result, which is usually referred to as the Euler-Fermat Theorem: it is due to Euler, but contains Fermat's First Theorem as a special case.

Theorem 3.29. *If a is an integer coprime to $m \ge 2$, then $a^{\varphi(m)} \equiv 1 \bmod m$.*

For $m = p$ prime, we have $\varphi(p) = p - 1$, and Euler's Theorem becomes Fermat's First Theorem.

Proof. Let $[r_i]$, $i = 1, \ldots, t = \varphi(m)$, denote the residue classes in $(\mathbb{Z}/m\mathbb{Z})^\times$. Then we claim that $[ar_1]$, …, $[ar_t]$ are pairwise distinct. In fact, assume that $[ar_i] = [ar_j]$ with $i \ne j$, that is, $ar_i \equiv ar_j \bmod m$. Since $\gcd(a, m) = 1$, we may cancel a, and get $[r_i] = [r_j]$: contradiction.

Since the classes $[ar_1]$, …, $[ar_t]$ are all in $(\mathbb{Z}/m\mathbb{Z})^\times$ and different, and since there are only t different classes in $(\mathbb{Z}/m\mathbb{Z})^\times$, we must have $(\mathbb{Z}/m\mathbb{Z})^\times = \{[ar_1], \ldots, [ar_t]\}$. But then $\prod_{i=1}^t [r_i] = \prod_{i=1}^t [ar_i] = [a]^{\varphi(m)} \prod_{i=1}^t [r_i]$. Since the $[r_i]$ are coprime to m, so is their product. Canceling then gives $[a]^{\varphi(m)} = [1]$, which proves the claim. □

The proofs of Fermat's First Theorem and that of the Theorem of Euler-Fermat have the same structure. In fact, the very same idea gives the following more general result known as

Theorem 3.30 (Lagrange's Theorem)**.** *Let G be a multiplicatively written finite abelian group with n elements. Then $g^n = 1$ for all $g \in G$.*

Proof. Write $G = \{g_1, \ldots, g_n\}$. Then the elements g_1g, …, g_ng are pairwise distinct: if we had $g_ig = g_jg$, then multiplying by the inverse of g yields $g_i = g_j$. Thus multiplication by g only permutes the elements, and we find (using the commutativity of G)

$$\prod_{j=1}^n g_j = \prod_{j=1}^n (g_jg) = g^n \prod_{j=1}^n g_j.$$

Multiplying through by the inverse of the product of all group elements gives $g^n = 1$. □

We remark that the result continues to hold for non-abelian groups, but that the proof has to be modified (see Exer. 2.6).

Lemma 3.31. *Let G be a finite cyclic group with n elements, and fix $g \in G$. Then the following statements are equivalent:*

1. *the order of g is equal to n;*
2. *the element g generates G, i.e., we have $G = \langle g \rangle$.*

Euler's Phi Function

For the application of Euler-Fermat we need a formula that allows us to compute $\varphi(n)$. Let us first compute $\varphi(n)$ directly for some small n. For $n = 6$, there are 6 different residue classes modulo 6; the classes [0], [2], [3] and [4] are not coprime to 6 (or, in other words, do not have a multiplicative inverse), which leaves the classes [1] and [5] as the only ones that are coprime to 6: thus $\varphi(6) = 2$. The classes mod 8 coprime to 8 are [1], [3], [5], [7], hence $\varphi(8) = 4$. If p is a prime number, then all the $p-1$ classes $[1]$, $[2]$, …, $[p-1]$ are coprime to p, hence $\varphi(p) = p-1$. In this way we can obtain the following table giving the values of $\phi(n)$ for small integers n.

n	3	4	5	6	7	8	9	10	12	15
$\varphi(n)$	2	2	4	2	6	4	6	4	4	8

We can easily compute $\varphi(p^k)$ (Euler's phi function for prime powers): starting with all the nonzero classes $[1]$, $[2]$, …, $[p^2-1]$ (there are p^2-1 of them) we have to eliminate those that are not coprime to p^2, that is, exactly the multiples of p smaller than p^2: these are p, $2p$, $3p$, …, $(p-1)p$ (note that $p \cdot p = p^2 > p^2-1$); since there are exactly $p-1$ of these multiples of p, there will be exactly $p^2-1-(p-1) = p^2-p = p(p-1)$ classes left: thus $\varphi(p^2) = p(p-1)$.

The same method works for general prime powers p^k: there are exactly p^k-1 nonzero classes, namely $[1]$, $[2]$, …, $[p^k-1]$. The multiples of p among these classes are $[p]$, $[2p]$, …, $[p^k-p] = [(p^{k-1}-1)p]$, and there are exactly $p^{k-1}-1$ of them. Thus $\varphi(p^k) = p^k-1-(p^{k-1}-1) = p^k-p^{k-1} = p^{k-1}(p-1)$.

We have proved

Proposition 3.32. *For primes p and integers $k \geq 1$, we have*

$$\varphi(p^k) = p^{k-1}(p-1).$$

Let us now compute $\varphi(pq)$ for a product of two different primes. We have $pq-1$ nonzero residue classes $[1]$, $[2]$, …, $[pq-1]$. The classes that have a factor in common with pq are multiples of p and multiples of q, namely $[p]$, $[2p]$, …, $[(q-1)p$ and $[q]$, $[2q]$, …, $[(p-1)q]$. Since there are no multiples of p that are multiples of q (like $[0]$, $[pq]$, etc) among these, there will be exactly $pq-1-(p-1)-(q-1) = pq-p-q+1 = (p-1)(q-1)$ classes left after eliminating multiples of p or q. Thus $\varphi(pq) = (p-1)(q-1) = \varphi(p)\varphi(q)$.

The general result is

Proposition 3.33. *If m and n are coprime integers, then $\varphi(mn) = \varphi(m)\varphi(n)$.*

Functions $f : \mathbb{N} \longrightarrow \mathbb{R}$ with the property that $f(mn) = f(m)f(n)$ whenever m and n are coprime are called **multiplicative functions**.

It is possible to prove Prop. 3.33 by generalizing the counting argument in the case of a product of two distinct primes. The proof we want to give, however, proceeds by constructing an isomorphism between groups that have order $\phi(mn)$ and $\phi(m) \cdot \phi(n)$, respectively. Before we turn to the proof, let us see how it works in a specific example like $m = 5$ and $n = 3$. What we'll do is take a residue class modulo 15 and coprime to 15, and map it to a pair of residue classes mod 3 and mod 5:

a mod 15	1	2	4	7	8	11	13	14
a mod 3	1	2	1	1	2	2	1	2
a mod 5	1	2	4	2	3	1	3	4

Thus we have the following pairs of residue classes modulo 3 and 5: $(1,1)$, $(1,2)$, $(1,3)$, $(1,4)$ and $(2,1)$, $(2,2)$, $(2,3)$, $(2,4)$. In particular, there are $\varphi(5) = 4$ pairs with $a \equiv 1 \bmod 3$ and 4 pairs with $a \equiv 2 \bmod 3$.

As we have promised above we now will construct an isomorphism between a group with order $\phi(mn)$ and one with order $\phi(m) \cdot \phi(n)$. The most natural choice is, of course, trying to find an isomorphism

$$\psi^\times : (\mathbb{Z}/mn\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times. \tag{3.1}$$

It is rather easy to write down such a homomorphism and to show that it is injective; for proving that an injective map between two finite groups is surjective it would be sufficient to show that both groups have the same number of elements, which is what we are trying to prove in the first place. A second option, which avoids counting arguments, is constructing an inverse map.

We will choose a third option and make the proof simpler by proving more. In fact we will construct a *ring homomorphism*

$$\psi : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, \tag{3.2}$$

and the very same arguments that we have just sketched will show that ψ is an injective homomorphism. But now surjectivity is clear since both $\mathbb{Z}/mn\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ have mn elements. What we have to prove in addition to the claims above is that the map ψ restricts to a map $\psi^\times$ between the unit groups of these rings, and that $\psi^\times$ is bijective if ψ is. But this is a simple exercise that works for general rings:

Fact 3.34. *If R and S are unital rings, and if $f : R \longrightarrow S$ is a ring homomorphism, then the restriction of f to the unit group $R^\times$ induces a group homomorphism $f^\times : R^\times \longrightarrow S^\times$. In addition, if f is injective (resp. bijective), then so is $f^\times$.*

Proof. We first show that if $u \in R^\times$ is a unit, then $f(u) \in S^\times$. But if $uv = 1$ in R, then $f(u)f(v) = f(uv) = f(1) = 1$ in S, and this shows that $f(u)$ is a unit. Since f is a ring homomorphism, its restriction to $R^\times$ must be a group homomorphism.

Now assume that f is injective, and suppose that $f^\times(u) = 1$. Then $f(u-1) = 0$, hence $u - 1 = 0$ by injectivity of f.

Finally, assume that f is bijective, and that $s \in S^\times$. Since s is a unit, there is an element $s' \in S$ with $ss' = 1$. Since f is surjective, there exist $r, r' \in R$ with $f(r) = s$ and $f(r') = s'$. But now $f(rr') = f(r)f(r') = ss' = 1$, and since f is injective we find $rr' = 1$ as above. Thus $r, r' \in R^\times$, and this finishes the proof. □

At this point we know that once we have an isomorphism (3.2) of rings, then the restriction $\psi^\times$ to the unit groups in (3.1) is an isomorphism of groups. In particular, the groups in question have equal orders, and this implies that ϕ is multiplicative as was claimed in Prop. 3.33. Thus it only remains to construct ψ and verify that it is an isomorphism of rings.

The most natural idea of defining a map as in (3.2) is sending a residue class modulo mn to the pair of residue classes modulo m and n:

$$\psi([a]_{mn}) = ([a]_m, [a]_n). \tag{3.3}$$

All that's left to do is check that it works. For proving that ψ is well defined we have to verify that if $[a]_{mn} = [b]_{mn}$, then $[a]_m = [b]_m$ and $[a]_n = [b]_n$. But this is clear since $a \equiv b \bmod mn$ clearly implies that $a \equiv b \bmod m$ and $a \equiv b \bmod n$.

It is also immediate that ψ is a ring homomorphism since

$$\psi([ab]_{mn}) = ([ab]_m, [ab]_n) = ([a]_m[b]_m, [a]_n[b]_n) = ([a]_m, [a]_n)([b]_m, [b]_n) = \psi([a]_{mn})\psi([b]_{mn}),$$

and the same calculation works for sums instead of products.

Next we show that ψ is injective. If $[a]_{mn} \in \ker \psi$ then $[a]_m = 0$ and $[a]_n = 0$, i.e., $m \mid a$ and $n \mid a$. Since $\gcd(m, n) = 1$, this implies that $mn \mid a$, which means that $[a]_{mn} = 0$. Thus $\ker \psi$ is trivial, and this is equivalent to injectivity.

Finally, surjectivity follows from the fact that the rings on both sides of (3.2) have the same cardinality, and the following

Fact 3.35. *If $f : R \longrightarrow S$ is an injective ring homomorphism, and if R and S are finite rings with the same cardinality, then f is an isomorphism.*

This is immediate from the fact that $\operatorname{im} f_+ \simeq R/\ker f_+$, where f_+ is the group homomorphism from the additive group of R to that of S: indeed the injectivity implies $\ker f_+ = 0$, and then we have $\operatorname{im} f_+ \simeq R$. Thus $|\operatorname{im} f_+| = |R| = |S|$ by the assumption that R and S have the same cardinality, hence f_+ is surjective as claimed.

Combining the formulas for Euler's phi function for prime powers and for products of coprime integers, we now find that an integer $m = p_1^{a_1} \cdots p_r^{a_r}$ has exactly

$$\begin{aligned}\varphi(m) &= (p_1 - 1)p_1^{a_1-1} \cdots (p_r - 1)p_r^{a_r-1} = p_1^{a_1} \cdots p_r^{a_r} \cdot \frac{p_1 - 1}{p_1} \cdots \frac{p_r - 1}{p_r} \\ &= m\Big(1 - \frac{1}{p_1}\Big) \cdots \Big(1 - \frac{1}{p_r}\Big)\end{aligned}$$

residue classes coprime to m, and we have proved

Proposition 3.36. *For positive integers $m = p_1^{a_1} \cdots p_r^{a_r}$ we have*

$$\phi(m) = m\Big(1 - \frac{1}{p_1}\Big) \cdots \Big(1 - \frac{1}{p_r}\Big).$$

The Chinese Remainder Theorem

In our proof of the multiplicativity of Euler's phi function we have constructed a map $\psi : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, whose definition was very natural in that it sent a residue class $[a]_{mn}$ modulo mn to the pair of residue classes $([a]_m, [a]_n)$ modulo m and modulo n. The fact that ψ is surjective was proved in a somewhat roundabout way, and it is desirable to find an explicitly given inverse map. Writing down such an inverse map is not exactly trivial: of course the pair $([a]_m, [a]_n)$ is the image of $[a]_{mn}$, but in general the residue classes in $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ will not do us the favor of being represented by one and the same integer a right from the start. Rather we will have to show how to find, given a pair of residue classes $([r]_m, [s]_n)$, a residue class $[a]_{mn}$ with $[a]_m = [r]_m$ and $[a]_n = [s]_n$. In terms of congruences this means that if we are given integers r and s and coprime moduli m and n, we have to find a solution of the pair of congruences

$$a \equiv r \bmod m, \qquad a \equiv s \bmod n.$$

Problems like this one were studied in Western Europe for centuries, often in connection with puzzles and recreational problems. Later it became known that methods for solving such congruences were already known in antiquity to Chinese mathematicians, and the corresponding result became known as the Chinese Remainder Theorem.

The idea behind the solution is quite simple: we have to show that, given residue classes $[r]_m$ and $[s]_n$, there exists a residue class $[a]_{mn}$ such that $[a]_m = [r]_m$ and $[a]_n = [s]_n$. At this point, Bezout comes to our rescue: since $\gcd(m, n) = 1$, there exist $x, y \in \mathbb{Z}$ such that $1 = mx + ny$. Now put $a = ryn + sxm$: then $a = ryn + sxm \equiv ryn \equiv 1 \bmod m$ since $yn \equiv 1 \bmod m$ from the Bezout representation, and similarly $a = ryn + sxm \equiv sxm \equiv s \bmod n$.

Here is how one could come up with the application of Bezout in the above proof. Given coprime residue classes $r \bmod m$ and $s \bmod m$, we want a formula for computing an integer a such that $a \equiv r \bmod m$ and $a \equiv s \bmod n$. The first idea is to see whether a can be written as a linear combination of r and s, that is, to look for integers x, y such that $a = xr + ys$. Reduction modulo m gives

$$r \equiv a = xr + ys \bmod m. \tag{3.4}$$

The simplest way to achieve this is by taking $x = 1$ and $y = 0$. But observe that we also need

$$s \equiv a \equiv xr + ys \bmod n. \tag{3.5}$$

Thus we need more leeway. The right idea is to observe that (3.4) will be satisfied whenever $x \equiv 1 \bmod m$ and $y \equiv 0 \bmod m$. Similarly, (3.5) will be satisfied if $x \equiv 0 \bmod n$ and $y \equiv 1 \bmod n$.

Is it possible to satisfy these four congruences simultaneously? Let's see: $x \equiv 0 \bmod n$ and $y \equiv 0 \bmod m$ mean $x = an$ and $y = bm$ for some $a, b \in \mathbb{Z}$. The two other congruences boil down to $x = an \equiv 1 \bmod m$ and $y = bm \equiv 1 \bmod n$. But these are both solvable since $\gcd(m, n) = 1$, so n has an inverse a modulo m, and m has an inverse b modulo n. Inverses can be computed using Bezout, and collecting everything we now can see where the formulas in the above proof were coming from.

Proposition 3.37. *Let m and n be coprime integers. Then the system of congruences*

$$a \equiv r \bmod m, \qquad a \equiv s \bmod n$$

has the solution $a = ryn + sxm$, where x and y are integers satisfying the Bezout relation $1 = mx + ny$.

Using induction, this may be generalized from two congruences to an arbitrary number of congruences modulo coprime integers:

Theorem 3.38 (Chinese Remainder Theorem)**.** *Let $m_1, \ldots, m_r$ denote pairwise coprime integers. Then*

$$\mathbb{Z}/m_1 \cdots m_r\mathbb{Z} \simeq \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z}.$$

In particular, we have

$$(\mathbb{Z}/m_1 \cdots m_r\mathbb{Z})^\times \simeq (\mathbb{Z}/m_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/m_r\mathbb{Z})^\times. \tag{3.6}$$

The last claim (3.6) follows from Prop. 1.29. We also remark that (3.6), in the case $r = 2$, can be formulated as $\mathcal{H}(\mathbb{Z}/m_1m_2\mathbb{Z}) \simeq \mathcal{H}(\mathbb{Z}/m_1\mathbb{Z}) \oplus \mathcal{H}(\mathbb{Z}/m_2\mathbb{Z})$. This will allow us to generalize the Chinese Remainder Theorem to arbitrary Pell conics.

3.5. Primitive Roots

Where we show that the group of coprime residue classes modulo primes are cyclic, and apply our results to find prime factors of Mersenne and Fermat numbers.

In this section we will investigate the order of elements in the coprime residue class groups $(\mathbb{Z}/m\mathbb{Z})^\times$. The main question we will answer is for which integers m there exist elements with maximal possible order: we already know that the order of an element divides the order $\phi(m)$ of the group, and now we will show that there is an element with order $\phi(m)$ if and only if $m = 1, 2, 4$ or m is a power of an odd prime.

Order of Elements

Assume that we are given an integer m and an integer a coprime to m. Recall that the smallest exponent $n > 0$ such that $a^n \equiv 1 \bmod m$ is called the order of $a \bmod m$; we write $n = \operatorname{ord}_m(a)$. Note that we always have $\operatorname{ord}_m(1) = 1$. Here is a table for the orders of elements in $(\mathbb{Z}/7\mathbb{Z})^\times$:

$a \bmod 7$	1	2	3	4	5	6
$\operatorname{ord}_7(a)$	1	3	6	3	6	2

If $m = p$ is prime, then Fermat's First Theorem gives us $a^{p-1} \equiv 1 \bmod p$, i.e., the order of $a \bmod p$ is at most $p - 1$. In general, the order of a is not $p - 1$; it is, however, always a divisor of $p - 1$ (as suggested by the table above):

Proposition 3.39. *Given a prime p and an integer a coprime to p, let n denote the order of a modulo p. If m is any integer such that $a^m \equiv 1 \bmod p$, then $n \mid m$. In particular, n divides $p - 1$.*

Proof. Write $d = \gcd(n, m)$ and $d = nx + my$; then $a^d = a^{nx+my} \equiv 1 \bmod p$ since $a^n \equiv a^m \equiv 1 \bmod p$. The minimality of n implies that $n \le d$, but then $d \mid n$ shows that we must have $d = n$, hence $n \mid m$. □

We now present a pretty application of Prop. 3.39 to prime divisors of **Mersenne numbers** $M_n = 2^n - 1$ and **Fermat numbers** $F_n = 2^{2^n} + 1$.

Corollary 3.40. *If p is an odd prime and if $q \mid M_p$, then $q \equiv 1 \bmod 2p$.*

Proof. It suffices to prove this for prime values of q (why?). So assume that $q \mid 2^p - 1$; then $2^p \equiv 1 \bmod q$. By Proposition 3.39, the order of 2 mod p divides p, and since p is prime, we find that $p = \operatorname{ord}_p(a)$.

On the other hand, we also have $2^{q-1} \equiv 1 \bmod p$ by Fermat's First Theorem, so Proposition 3.39 gives $p \mid (q - 1)$, and this proves the claim because we clearly have $q \equiv 1 \bmod 2$. □

The following table lists a few small prime factors of Mersenne numbers $M_p = 2^p - 1$:

p	small factors
11	$23 = 2p + 1,\ 89 = 8p + 1$
23	$47 = 2p + 1$
29	$229 = 8p + 1,\ 1103 = 38p + 1$
37	$223 = 6p + 1$

Fermat numbers are integers of the form $F_n = 2^{2^n} + 1$: $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537, \ldots$; Fermat conjectured that these integers are all primes, based on the fact that he could exclude most of its possible divisors using the following result:

Corollary 3.41. *If q divides F_n, then $q \equiv 1 \bmod 2^{n+1}$.*

Proof. It is sufficient to prove this for prime divisors q. Assume that $q \mid F_n$; then $2^{2^n} + 1 \equiv 1 \bmod q$, hence $2^{2^n} \equiv -1 \bmod q$ and $2^{2^{n+1}} \equiv 1 \bmod q$. We claim that actually $2^{n+1} = \operatorname{ord}_q(2)$: in fact, Proposition 3.39 says that the order divides 2^{n+1}, hence is a power of 2. But 2^{n+1} is clearly the smallest power of 2 that does it.

On the other hand, $2^{q-1} \equiv 1 \bmod q$ by Fermat's First Theorem, and Proposition 3.39 gives $2^{n+1} \mid (q - 1)$, which proves the claim. □

Actually we can improve this: since $F_n \equiv 1 \bmod 8$ for $n \ge 2$ we know that $(2/F_n) = +1$, hence $2^{(q-1)/2} \equiv 1 \bmod q$, and now $2^{n+1} \mid \frac{q-1}{2}$, which shows

Corollary 3.42. *If q divides F_n, then $q \equiv 1 \bmod 2^{n+2}$.*

In particular, the possible prime divisors of $F_5 = 4294967297$ all have the form $q = 128m + 1$. After a few trial divisions one finds $F_5 = 641 \cdot 6700417$. This is how Euler disproved Fermat's conjecture. Today we know the prime factorization of F_n for all $n \le 11$, we know that F_n is composite for $5 \le n \le 30$ (and several larger values up to $n = 382447$), and we don't know any factors for $n = 14, 20, 22$ and 24.

Existence of Primitive Roots

Consider the multiplicative group $(\mathbb{Z}/m\mathbb{Z})^\times$ of the ring $\mathbb{Z}/m\mathbb{Z}$. Since $a^{\varphi(m)} \equiv 1 \bmod m$ for all $a \in (\mathbb{Z}/m\mathbb{Z})^\times$, the order of every such a divides $\varphi(m)$. It is natural to ask whether this is best possible, i.e., whether there exists an element $g \in (\mathbb{Z}/m\mathbb{Z})^\times$ with maximal possible order $\operatorname{ord}_m(g) = \varphi(m)$.

In a multiplicatively written group G, the powers a^n $(n \in \mathbb{Z})$ of an element form a subgroup of G, which we will denote by $\langle a \rangle$. In the group $G = (\mathbb{Z}/7\mathbb{Z})^\times$, for example, the subgroups generated by its elements are

a	1	2	3	4	5	6
$\langle a \rangle$	$\{1\}$	$\{1,2,4\}$	G	$\{1,2,4\}$	G	$\{1,6\}$

Thus $G = \langle 3 \rangle$ and $G = \langle 5 \rangle$, whereas the other elements generate subgroups of orders 1, 2 or 3.

As the example $m = 8$ shows, where $\varphi(m) = 4$, but $\operatorname{ord}_8(a) \le 2$ for all $a \in (\mathbb{Z}/8\mathbb{Z})^\times$ (remember that $a^2 \equiv 1 \bmod 8$ for all odd integers a), this is not true. On the other hand, $\operatorname{ord}_3(2) = 2 = \varphi(3)$, $\operatorname{ord}_5(2) = 4 = \varphi(5)$, and $\operatorname{ord}_7(3) = 6 = \varphi(7)$ show that elements of maximal possible order exist for all small primes.

Elements $g \in (\mathbb{Z}/m\mathbb{Z})^\times$ with $\operatorname{ord}_m(g) = \varphi(m)$ are called **primitive roots** modulo m.

Fact 3.43. *The following statements are equivalent:*

1. *g is a primitive root modulo m;*
2. *every $a \in (\mathbb{Z}/m\mathbb{Z})^\times$ can be written in the form $a \equiv g^k \bmod m$ for some integer k;*
3. *the residue class $[a]_m$ has order $\phi(m)$ in $(\mathbb{Z}/m\mathbb{Z})^\times$;*
4. *$(\mathbb{Z}/m\mathbb{Z})^\times$ is a cyclic group generated by g.*

We will now prove that there always exist primitive roots modulo primes p. In our proof we will need the following

Lemma 3.44. *For every $n \in \mathbb{N}$ we have $\sum_{d \mid n} \varphi(d) = n$.*

For $n = 6$ this says $\varphi(1) + \varphi(2) + \varphi(3) + \varphi(6) = 1 + 1 + 2 + 2 = 6$.

Proof. Consider the fractions $\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n}{n}$. For some $d \mid n$, how many of these fractions have denominator d when written in lowest terms?

Clearly there will be $\varphi(n)$ fractions with denominator n since these are exactly the $\frac{k}{n}$ with $\gcd(k, n) = 1$. Now assume that $n = dm$; the fraction $\frac{k}{n}$ will have denominator d if and only if $k = mt$ and $\gcd(t, d) = 1$. Clearly there are $\varphi(d)$ such fractions.

Thus among the n fractions, for each $d \mid n$ there are $\varphi(d)$ fractions with denominator d, hence $n = \sum_{d \mid n} \varphi(n)$. □

For computing the order of elements in residue classes we use the following simple lemma, which puts bounds on the order of a product of elements.

Lemma 3.45. *Let G be a finite cyclic group of order n generated by g. Then the order of g^k is $\frac{n}{\gcd(d,k)}$.*

Proof. We have $(g^k)^{d/\gcd(d,k)} = (g^{k/\gcd(d,k)})^d = 1$, so the order of g^k divides $d/\gcd(d,k)$. On the other hand, from $1 = (g^k)^m = g^{km}$ we deduce that $d \mid km$, since d is the order of g. Dividing through by $\gcd(d,k)$ gives $\frac{d}{\gcd(d,k)} \mid \frac{k}{\gcd(d,k)} m$. But since $\frac{d}{\gcd(d,k)}$ and $\frac{k}{\gcd(d,k)}$ are coprime (we have divided out the common factors), this implies that $\frac{d}{\gcd(d,k)} \mid m$, which proves our claim. □

Gauss's idea for proving the existence of primitive roots can be expressed as follows:

Proposition 3.46. *Let G be a finite group. Assume that, for every divisor d of $n = \#G$, the equation $x^d = 1$ has at most d solutions. Then G is cyclic.*

Proof. Assume that $d \mid n$, and let $\psi(d)$ denote the number of elements in G with order d (thus for $G = (\mathbb{Z}/5\mathbb{Z})^\times$, we have $\psi(1) = 1$, $\psi(2) = 1$, and $\psi(4) = 2$). If $\psi(d) \neq 0$, then there is an element $g \in G$ of order d, and then $1, g, g^2, \ldots, g^{d-1}$ are distinct solutions of the equation $x^d = 1$ in G. By assumption, there are at most that many solutions, hence these are all solutions of $x^d = 1$.

Now if g has order d, then by Lemma 3.45 there are exactly $\varphi(d)$ elements of order d in the group $H = \langle g \rangle$ generated by g, namely the g^k with $\gcd(d,k) = 1$. In other words: we either have $\psi(d) = 0$ or $\psi(d) = \varphi(d)$.

Clearly every element of g has some order, and this order divides $n = \#G$, hence $n = \sum_{d|n} \psi(d)$ (in the example $G = (\mathbb{Z}/5\mathbb{Z})^\times$ used above, there are 4 elements, namely one with order 1, one with order 2, and two with order 2, hence $4 = 1 + 1 + 2$). Next $\psi(d) \leq \varphi(d)$ implies that $n = \sum_{d|n} \psi(d) \leq \sum_{d|n} \varphi(d) = n$, where we have used that $\sum_{d|n} \varphi(d) = n$. We now see that we must have equality in $\sum_{d|n} \psi(d) \leq \sum_{d|n} \varphi(d)$. But this happens if and only if $\psi(d) = \varphi(d)$ for every $d \mid n$, and in particular there exists an element of order n since $\psi(n) = \varphi(n) \geq 1$. □

We will sketch another proof of Prop. 3.46 in Exer. 3.18.

Theorem 3.47. *For every prime number p, there exist exactly $\varphi(p-1)$ primitive roots modulo p.*

In particular, there are $2 = \varphi(6)$ primitive roots modulo 7 (namely 3 and 5), and there are $4 = \varphi(10)$ primitive roots modulo 11.

For proving Thm. 3.47 we have to show that for every $d \mid (p-1)$, there are at most d solutions of the congruence $x^d \equiv 1 \bmod p$. Equivalently, the polynomial $X^d - 1$ has at most d roots over the field $\mathbb{Z}/p\mathbb{Z}$. This is a special case of the following

Theorem 3.48. *Let R be a domain. Then a polynomial $f \in R[T]$ has at most* $\deg f$ *roots in R.*

This result does not hold in general rings: the polynomial $T^2 - 1$ in $(\mathbb{Z}/8\mathbb{Z})[T]$, for example, has four roots, namely ± 1 and ± 3. It is still possible to factor out the corresponding linear terms, since

$$T^2 - 1 = (T-1)(T+1) = (T-3)(T+3)$$

in $(\mathbb{Z}/8\mathbb{Z})[T]$, yet 3 is not a root of the factors $T-1$ or $T+1$ in the first factorization of T^2-1. This example, by the way, shows that $(\mathbb{Z}/8\mathbb{Z})[T]$ does not have unique factorization: the factors $T-a$ of T^2-1 for $a \in (\mathbb{Z}/8\mathbb{Z})^\times$ are neither units nor associated, hence T^2-1 has two essentially distinct factorizations.

It *is* true, however, that if a is a root of f, then f can be written in the form $f(T) = (T-a) \cdot g(T)$ for some polynomial g. This is what we will prove next:

Proposition 3.49. *Let R be a ring, and let $f \in R[T]$ be a polynomial. If $f(a) = 0$ for some $a \in R$, then there exists a polynomial $g \in R[T]$ such that $f(T) = (T-a)g(T)$.*

Proof. Our proof uses the fact that

$$T^n - a^n = (T-a)(T^{n-1} + aT^{n-2} + \ldots + a^{n-2}T + a^{n-1}). \tag{3.7}$$

Writing $f(T) = a_nT^n + \ldots + a_1T + a_0$ we get

$$\begin{aligned} f(T) = f(T) - f(a) &= a_n(T^n - a^n) + a_{n-1}(T^{n-1} + a^{n-1}) + \ldots + a_1(T-a) \\ &= (T-a)g(T), \end{aligned}$$

where we have used the observation that all the expressions inside the brackets on the right hand side are divisible by $T-a$ because of (3.7). □

Now Thm.3.48 can be proved by induction. We may assume without loss of generality that $f \in K[T]$ is a monic polynomial. Clearly linear polynomials $T-a$ have a single root a. Assume the claim holds for all polynomials of degree $< n$, and let $f \in K[T]$ be a polynomial with degree n. If f has no root, the claim is trivially true. If $f(a) = 0$, then $f(T) = (T-a)g(T)$, where g has degree $< n$. Assume that f has a root b with $b \ne a$. Then $(b-a)g(b) = 0$, and since K is a domain (even a field), we may deduce that $g(b) = 0$. Thus every root $b \ne a$ of f is a root of g, and by induction assumption there are at most $\deg g = n-1$ such roots. This implies the claim.

With this result, our proof of the existence of primitive roots modulo primes (Thm. 3.47) is complete.

Let us also observe that the existence of primitive roots allows us to give a second proof of the following fact already shown in Prop. 3.5 and Prop. 3.21:

Corollary 3.50. *For odd prime numbers p, the congruence $x^2 \equiv -1 \bmod p$ is solvable if and only if $p \equiv 1 \bmod 4$.*

Proof. Assume that $x^2 \equiv -1 \bmod 4$; raising this congruence to the $\frac{p-1}{2}$-th power and using Fermat's First Theorem implies $1 \equiv (-1)^{(p-1)/2} \bmod p$, which shows that $\frac{p-1}{2}$ is even and thus $p \equiv 1 \bmod 4$.

Conversely assume that $p \equiv 1 \bmod 4$ and write $p = 4n+1$. Let g denote a primitive root modulo p; we claim that $g^{2n} \equiv -1 \bmod p$. In fact since $g^{4n} = g^{p-1} \equiv 1 \bmod p$ we must have $g^{2n} \equiv \pm 1 \bmod p$, but since g is a primitive root and has order $p-1 = 4n$ we must have $g^{2n} \equiv -1 \bmod p$. Now $x = g^n$ is a solution of the congruence Then $x^2 \equiv -1 \bmod p$. □

We remark that the existence of primitive roots modulo primes p can also be formulated in a more abstract way: there is a primitive root modulo n if and only if the group $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic. In fact, primitive roots modulo p are, by definition, generators of the cyclic group $(\mathbb{Z}/p\mathbb{Z})^\times$. Thus the existence of a primitive root modulo primes p is equivalent to an isomorphism $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$. We can construct such an isomorphism by choosing a primitive root g modulo p; then we define a homomorphism

$$\lambda : \mathbb{Z}/(p-1)\mathbb{Z} \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times \quad \text{by} \quad \lambda(a) = [g^a]_p.$$

Checking that this is a well-defined homomorphism and showing that is bijective is an easy exercise.

This isomorphism λ depends on the choice of the primitive root; such isomorphisms are called non-canonical isomorphisms.

Next we claim that there are primitive roots modulo all odd prime powers; again this may be formulated as an isomorphism between $(\mathbb{Z}/p^n\mathbb{Z})^\times$ and a cyclic group with $\phi(p^n) = (p-1)p^{n-1}$ elements:

Theorem 3.51. *If p is an odd prime number and $n \geq 1$ an integer, then there exist primitive roots modulo p^n. More exactly we have*

$$(\mathbb{Z}/p^n\mathbb{Z})^\times \longrightarrow \mathbb{Z}/(p-1)p^{n-1}\mathbb{Z}.$$

Observe that $(\mathbb{Z}/2p^n\mathbb{Z})^\times \simeq (\mathbb{Z}/p^n\mathbb{Z})^\times$ by the Chinese Remainder Theorem, hence there also are primitive roots modulo $2p^n$ for odd primes p and exponents $n \geq 1$.

We will prove Thm. 3.51 using the technique of "divide and conquer". For showing that the group $(\mathbb{Z}/p^n\mathbb{Z})^\times$ of order $(p-1)p^{n-1}$ is cyclic we split it up into two groups of order $p-1$ and p^{n-1}: we claim that there is an exact sequence

$$\begin{tikzcd} 1 \arrow[r] & A \arrow[r] & (\mathbb{Z}/p^n\mathbb{Z})^\times \arrow[r, "\pi"'] & (\mathbb{Z}/p\mathbb{Z})^\times \arrow[r] & 1 \end{tikzcd} \tag{3.8}$$

with $\#A = p^{n-1}$.

This is easy. The canonical projection defined by $\pi(a + p^n\mathbb{Z}) = a + p\mathbb{Z}$ is a surjective group homomorphism $(\mathbb{Z}/p^n\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$. Its kernel A consists of all residue classes $a + p^n\mathbb{Z}$ with $a \equiv 1 \bmod p$. Since $\#(\mathbb{Z}/p^n\mathbb{Z})^\times = (p-1)p^{n-1}$ and $\#(\mathbb{Z}/p\mathbb{Z})^\times = p-1$, the kernel A must have order p^{n-1}

Next we observe that it is sufficient to show that A is cyclic. This is due to the following observation:

Lemma 3.52. *If*

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r] & G \arrow[r] & B \arrow[r] & 0 \end{tikzcd}$$

is an exact sequence of finite abelian groups, and if A and B are cyclic with coprime orders $\#A = a$ and $\#B = b$, respectively, then $G \simeq \mathbb{Z}/ab\mathbb{Z}$ is cyclic.

Proof. Let g be a generator of A and $h'A$ a generator of $B \simeq G/A$. Then $(h')^b \in A$, hence $h = (h')^a$ satisfies $h^b = 1$. Moreover, hA also generates B since the map $x \to x^a$ is an automorphism of B by Fact 2.1.

Now write $am + bn = 1$ for integers m, n; we claim that g^nh^m has order ab. Clearly $(g^nh^m)^{ab} = 1$, so the order of g^nh^m divides ab. Assume therefore that $(g^nh^m)^k = 1$. Then $(g^nh^m)^a = g^{an}h^{am} = h^{am} = h^{1-bn} = h$, hence $1 = (g^nh^m)^{ak} = h^k$. Since h has order b, we deduce that $b \mid k$. Similarly, $(g^nh^m)^b = g^{nb}h^{mb} = g^{nb} = g^{1-am} = g$, hence $1 = (g^nh^m)^{bk} = g^k$, which shows that $a \mid k$. Since $\gcd(a, b) = 1$, this implies $ab \mid k$, and the claim follows. □

Thus for proving Thm. 3.51 it is sufficient to show that the kernel

$$A = \ker \pi = \{a + p^n\mathbb{Z} : a \equiv 1 \bmod p\}$$

of the projection map π in (3.8) is cyclic. We claim that $a = 1 + p$ has order p^{n-1}, which implies the claim. In fact we have $a^{p^k} \equiv 1 + p^k \bmod p^{k+1}$ for $0 \leq k \leq n-1$. This is true for $k = 0$, and if it holds for some k, then $a^{p^{k+1}} = (1 + p^k + rp^{k+1})^p \equiv 1 + p^{k+1} \bmod p^{k+2}$.

This completes the proof of Thm. 3.51. The analogous result for powers of 2 is the following:

Proposition 3.53. *The coprime residue class group $(\mathbb{Z}/2^k\mathbb{Z})^\times$ is cyclic if and only if $k \leq 2$. For $k \geq 3$, the group $(\mathbb{Z}/2^k\mathbb{Z})^\times$ is generated by the residue classes represented by -1 and 5. More exactly, we have*

$$(\mathbb{Z}/2^k\mathbb{Z})^\times \simeq \begin{cases} 0 & \textit{if } k = 1, \\ \mathbb{Z}/2\mathbb{Z} & \textit{if } k = 2, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^{k-2}\mathbb{Z} & \textit{if } k \geq 3. \end{cases}$$

Proof. Clearly $(\mathbb{Z}/2\mathbb{Z})^\times = \langle[1]\rangle$ and $(\mathbb{Z}/4\mathbb{Z})^\times = \langle[-1]\rangle$ are cyclic. The group $(\mathbb{Z}/8\mathbb{Z})^\times$ is not cyclic since the elements [3], [5] and [7] all have order 2. But it is easily checked that every coprime residue class $a \bmod 8$ can be written uniquely in the form $a \equiv (-1)^r \cdot 5^s \bmod 8$ for $0 \le r, s \le 1$. Now we claim that the residue classes $(-1)^r 5^s \bmod 2^n$ (for $n \ge 3$) are pairwise distinct for $0 \le r \le 1$ and $0 \le s \le 2^{n-2}$. Assuming the truth of this statement for the moment, we see that there are 2^{n-1} distinct coprime residue classes modulo 2^n represented by the powers of -1 and 5, and then the claim follows since $2^{n-1} = \varphi(2^n)$.

Suppose therefore that $(-1)^r 5^s \equiv (-1)^t 5^u \bmod 2^n$ for integers $0 \le r, t \le 1$ and $0 \le s, u \le 2^{n-2}$. Then $(-1)^r \equiv (-1)^t \bmod 4$ shows that $r \equiv t \bmod 2$, which implies $r = t$. Thus $5^s \equiv 5^u \bmod 2^n$, or $2^n \mid (5^{s-u} - 1)$. Since $n \ge 3$ we see that s and u have the same parity, i.e., are either both even or both odd. Thus $s-u = 2k$, and $2^n \mid (5^{2k}-1) = (5^k-1)(5^k+1)$. Since the second factor is $5^k + 1 \equiv 2 \bmod 4$, the last divisibility relation is equivalent to $2^{n-1} \mid (5^k - 1)$. □

We have used the following

Lemma 3.54. *We have* $5^{2^{k-2}} \equiv 1 + 2^{k-1} \bmod 2^k$ *for all* $k \ge 3$.

Proof. For $k = 3$ we have $5^2 \equiv 1 + 2^3 \bmod 2^4$ as claimed. Assume that the claim holds for some integer $k \ge 3$; then $5^{2^{k-2}} = 1 + 2^{k-1} + 2^k q$ for some integer q, and squaring yields

$$\begin{aligned} 5^{2^{k-1}} &= (1 + 2^{k-1} + 2^k q)^2 = 1 + 2^k + 2^{2k-2} + 2^{k+1}q + 2^{2k}q + 2^{2k}q^2 \\ &= 1 + 2^k \bmod 2^{k+1} \end{aligned}$$

as long as $k \ge 3$. □

Finally we show

Theorem 3.55. *There exists a primitive root modulo* $m \in \mathbb{N}$ *if and only if*

$$m = 1, 2, 4, p^n, 2p^n,$$

where p *is an odd prime number and* n *is an arbitrary positive integer.*

For the proof we use the following

Lemma 3.56. *Let* G *and* H *be finite cyclic groups of orders* $\#G = m$ *and* $\#H = n$. *Then the group* $G \oplus H$ *is cyclic if and only if* $\gcd(m, n) = 1$.

Proof. Assume that $G \oplus H = \langle(g, h)\rangle$ is generated by the element (g, h). Then (g, h) has order mn, hence $(g, h)^m = (g^m, h^m) = (1, h^m)$ has order n. But then h^m has order n in H, and this is only possible if m and n are coprime.

Now assume conversely that $\gcd(m, n) = 1$. Let $g \in G$ and $h \in H$ be elements with $G = \langle g\rangle$ and $H = \langle h\rangle$, and assume that $(g, h)^k = (1, 1)$. Then $g^k = 1$ in G and $h^k = 1$ in H, so k must be a multiple of both m and n. Since these numbers are coprime, k is a multiple of mn, and this shows that (g, h) has order mn. □

Now we can finish the proof of Thm. 3.55. Assume that $(\mathbb{Z}/m\mathbb{Z})^\times$ is cyclic. If m can be factored as $m = ab$ for coprime integers $a, b \ne 1$, then $(\mathbb{Z}/m\mathbb{Z})^\times \simeq (\mathbb{Z}/a\mathbb{Z})^\times \oplus (\mathbb{Z}/b\mathbb{Z})^\times$ is not cyclic by the preceding lemma except whenever both $\varphi(a)$ and $\varphi(b)$ are even. This implies that m cannot be divisible by two distinct primes, or by an odd prime and 4. This leaves only the possibilities listed above, and for these cases we already know that primitive roots exist.

Primitive roots may be used for proving several basic results. Let us start with

Lemma 3.57. *If* g *denotes a primitive root modulo* p, *then* $(\frac{a}{p}) = +1$ *if and only if* $a \equiv g^{2k} \bmod p$ *for some* k, *and* $(\frac{a}{p}) = -1$ *if and only if* $a \equiv g^{2k+1} \bmod p$.

We can also prove Euler's criterion using primitive roots: If $a \equiv b^2 \bmod p$, then $a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \bmod p$ by Fermat's First Theorem as before.

If a is not congruent to a square modulo p, then $a \equiv g^{2n+1}$ is congruent to an odd power of a primitive root g modulo p, and $a^{\frac{p-1}{2}} \equiv g^{(2n+1)\cdot\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} \equiv -1 \bmod p$.

Notes

Various mathematicians have tried to come up with graphics that reflect certain structural properties of Abelian groups with small order. I am thinking in particular about D. Shanks [Sha1962]; the pictures used in the text for displaying multiplication modulo m come from Dynkin & Uspensky [DU1979]. Graphical representations of multiplication in residue classes go back to Poinsot and Hofmann [Hof188?].

The Chinese Remainder Theorem was known in Europe very early on, be it in connection with puzzles (see Bachet [Ba1612]) or as a basic result in number theory (Euler). It received its name rather late after the contributions of the Chinese mathematicians became known through the work of Biernatzki [Bie1856] and others. Linear indeterminate equations already showed up in the work of Hindu mathematicians such as Aryabhata, Brahmagupta and Bhaskara.

Fermat gave a special case of what we have called Fermat's First Theorem in a letter[3] to Mersenne written around June 1640:

> Let the numbers a unit smaller than those proceeding by double proportions, such as
>
> | | | | | | | | | | | |
> |---|---|---|---|---|---|---|---|---|---|---|
> | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
> | 1 | 3 | 7 | 15 | 31 | 63 | 127 | 255 | 511 | 1023 | 2047, |
>
> be called the radicals of the perfect numbers, because, every time they are prime, they produce perfect numbers. Put on top of these numbers in natural progression: 1, 2, 3, 4, 5, etc., which will be called their exponents.
> With these assumptions I say that:
> 1. If the exponent of a radical number is composite, its radical is also composite. For example, because the exponent 6 of the radical 63 is composite, I say that 63 is also composite.
> 2. If the exponent is a prime number, I say that its radical minus 1 is measured by the double of the exponent. For example since the exponent 7 of 127 is prime, I say that 126 is a multiple of 14.
> 3. If the exponent is a prime number, I say that its radical is only divisible by numbers that surpass by a unit the multiples of the double of the exponent. For example, since the exponent 11 of 2047 is prime, I say that it cannot be divisible by any number except those that are a unit greater than 22, such as 23, or a unit greater than a multiple of 22; in fact, 2047 is only divisible by 23 and 89, which, if you subtract a unit, gives 88, a multiple of 22.

In this letter Fermat only stated his results; later he claimed to have proofs, and there can be no doubt that he had such proofs. The first published proofs, however, are due to Leibniz (using the multinomial expansion of $(a+b+c+\ldots)^p$) and, in particular, Euler, who gave four different proofs. Proofs were also given by Lagrange, Lambert, Laplace (in Lacroix's *Traité du calcul différentiel et intégral*, vol.III, p. 722), Gauss, Dirichlet, and Poinsot.

Fermat also knew applications of his theorem on the forms of prime divisors of numbers such as $M_p = 2^p - 1$ and $F_n = 2^{2^n} + 1$. Again, the first proofs were given by Euler.

[3] This letter can be found on pp. 195–199 in vol. II of Fermat's Œuvres.

Fermat's conjecture on the primality of Fermat numbers was disproved by Euler, who found that $641 \mid F_5$. These integers became more interesting when Gauss succeeded in proving that a regular p-gon, where p is an odd prime, can be constructed with ruler and compass if p is a Fermat prime. Gauss also stated that he had proved the converse, namely that if a regular p-gon can be constructed by ruler and compass, then p is a Fermat prime, but the first proof was published by Pièrre Wantzel.

The theorem that primes of the form $4n + 1$ can be written as a sums of two squares was first stated by Girard, and first proved by Fermat, although the first published proof is due to Euler. Fermat also knew that primes are represented uniquely as sums of two squares, and even gave formulas for the number of representations of positive integers n as sums of two squares.

Euler's criterion

Lemma 3.44 is given by Gauss in his Disquisitiones [Gau1801, art. 39]; the proof we have given is credited by Wertheim [Wer1902, p. 48] to an oral communication from Emil Strauss.

Prop. 3.22 was published by Thue in 1902 in the following form: given any pair of integers coprime to some integer $p > 1$, there exist integers α, β, h and k such that $aq = \alpha p + h$ and $bq = \beta p + k$ with $0 < h^2, k^2 < p$. In other words: there is an integer q such that both aq and bq have "small" remainders when divided by p.

Vandiver [Van1915] credits the result to G.D. Birkhoff. A. Brauer & Reynolds [BR1951] have shown that the special case was already known to Aubry, a generalization of it to Vinogradov. The general statement is often credited to Scholz.

Exercises

3.1 Euler's additive proof of Fermat's First Theorem uses binomial coefficients: these are the entries in Pascal's triangle, and they occur in the binomial theorem

$$(a+b)^n = a^n + \binom{n}{1} a^{n-1}b + \binom{n}{2} a^{n-2}b^2 + \ldots + \binom{n}{n-1} ab^{n-1} + b^n.$$

1. Show that $\binom{n}{k} = \frac{n!}{k!(n-k)!}$,
2. Show that, for primes p, the numbers $\binom{p}{k}$, $k = 1, 2, \ldots, p-1$, are all divisible by p.
3. Show that the last claim does not hold in general for nonprimes, for example by computing $\binom{6}{2}$.
4. Show that Fermat's First Theorem is equivalent to the statement that $a^p \equiv a \bmod p$ for all $a \in \mathbb{Z}$. Hint: use induction on a.

3.2 The following proof of Fermat's First Theorem goes back to Leibniz:

1. Prove the Multinomial Theorem
$$(x_1 + x_2 + \ldots + x_r)^n = \sum \binom{n}{a_1\ a_2\ \ldots\ a_r} x_1^{a_1} x_2^{a_2} \cdots x_r^{a_r}, \tag{3.9}$$
where the sum is over all numbers $0 \le a_j \le n$ with $a_1 + a_2 + \ldots + a_r = n$.
2. Show that
$$\binom{n}{a_1\ a_2\ \ldots\ a_r} = \frac{n!}{a_1!\, a_2! \cdots a_r!}.$$
3. Show that all the multinomial coefficients occurring in (3.9) are divisible by p except those for which $a_j = p$ for some j and $a_i = 0$ for $i \ne j$.
4. Prove Fermat's First Theorem $r^p \equiv r \bmod p$ by setting $x_1 = x_2 = \ldots = x_r = 1$.

3.3 Find all integers with $\varphi(m) = 6$.

3.4 Show that m is prime if and only if $\varphi(m) = m - 1$.

3.5 Solve the system of congruences

$$x \equiv 12 \bmod 13,$$
$$x \equiv 7 \bmod 19.$$

3.6 Determine the orders of all elements in $(\mathbb{Z}/15\mathbb{Z})^\times$.

3.7 Compute $\varphi(180)$.

3.8 Let $n \equiv 7 \bmod 8$ be a positive integer. Show that n cannot be written as a sum of three squares.

3.9 Prove or disprove: $\varphi(n^2) = n(n-1)$ for every integer $n \geq 2$.

3.10 Use Cor. 3.41 for showing that for every integer $n > 1$, there are infinitely many primes $p \equiv 1 \bmod 2^n$.

3.11 Given a prime number p, use Cor. 3.40 for proving the existence of a prime $q \equiv 1 \bmod p$. For getting the existence if infinitely many such primes, generalize Cor. 3.40 to primitive factors of numbers $2^{p^n} - 1$: these are factors that do not divide any numbers $2^q - 1$ for $q < p^n - 1$.

3.12 (Form the first round of the German mathematical olympiad 2006; it is the traditionally "easy" first problem).
Find two consecutive integers with the property that the sum of their digits is each divisible by 2006.

3.13 Let $p \neq 2, 5$ be a prime; let r denote the period length of the decimal expansion of $\frac{1}{p}$.

1. compute the period length r for the primes $p = 7$, 11, 13, and 37. Observations?
2. Let $x = \frac{1}{p}$. Compare the decimal expansion of $10^r x$ with that of x and conclude that $10^r x - x$ is an integer.
3. Show that $10^r \equiv 1 \bmod p$.
4. Prove that r divides $p - 1$.

3.14 Is 2 a primitive root modulo 17?

3.15 Find the $4 = \varphi(10)$ primitive roots modulo 11.

3.16 Show that 4 is not a primitive root for any odd prime p.

3.17 Is there a primitive root modulo 12? If yes, give one; if no, why not?

3.18 (Lüneburg [Lue1978, p. 36]). Prove Prop. 3.46 as follows:

1. Let G be a finite abelian group. If $a, b \in G$ have order m and n, respectively, then there is an element $g \in G$ with order $\mathrm{lcm}(m, n)$.
2. If G is a finite abelian group, and if d is the maximal order of all elements in G, then $g^d = 1$ for all elements in G.
3. Prove Prop. 3.46 by observing that if d is the maximal order of all elements in G, then $x^d = 1$ has $n = \# G$ solutions in G. Deduce that $n \leq d \leq \# G$, and that we must have equality throughout.

3.19 For primes p and integers a, b, c, d with $0 \leq b, d < p$ show that the congruence

$$\binom{ap+b}{cp+d} \equiv \binom{a}{c}\binom{b}{d} \bmod p$$

holds.

3.20

1. Compute the order $\mathrm{ord}_p(10)$ of 10 mod p for the primes $p = 3$, 7, and 11, and complete the table below.

p	3	7	11	13	17	19
$\mathrm{ord}_p(10)$				6	16	18

2. For which of these primes is 2 a primitive root?

3. The following table gives the decimal expansion of $1/p$ for the primes $p \nmid 10$ up to 19 (the bar denotes periodicity):

$$\begin{aligned} 1/3 &= .\overline{3} \\ 1/7 &= .\overline{142857} \\ 1/11 &= .\overline{09} \\ 1/13 &= .\overline{076923} \\ 1/17 &= .\overline{0588235294117647} \\ 1/19 &= .\overline{052631578947368421} \end{aligned}$$

Compare the length of the period with your table above. What is the pattern?
* Prove your conjecture.

3.21 Denote the order of $g \in G$ (the smallest exponent $n > 1$ with $g^n = 1$) by $\operatorname{ord}(g)$. Let G be a finite abelian group. If $\operatorname{ord}(g) = m$ and $\operatorname{ord}(h) = n$ for $g, h \in G$, then

$$\frac{mn}{\gcd(m,n)} \mid \operatorname{ord}(gh) \mid mn.$$

3.22 Assume that $2^{n-1} \equiv 1 \bmod n$ for some odd integer n. Put $N = 2^n - 1$ and show that $2^N \equiv 1 \bmod N$.

3.23 A composite integer n is called a 2-pseudoprime if $2^n \equiv 1 \bmod p$. Show that there are infinitely many 2-pseudoprimes (Hint: $2^{11} - 1 = 23 \cdot 89$).

3.24 Show that for each integer $a \ge 2$ there exist infinitely many Fermat a-pseudoprimes.
Hint: Let p be a prime not dividing $a^2 - 1$; show that $n = (a^{2p} - 1)/(a^2 - 1)$ is composite and passes the Fermat test to base a.

3.25 Let $p \equiv 1 \bmod 3$ be a prime, and let g be a primitive root mod p. Show that, for $x = g^{(p-1)/3}$, we have $x^3 \equiv 1 \bmod p$ and $x \not\equiv 1 \bmod p$.

3.26 Let $p \equiv 1 \bmod 3$ be a prime, and let x be as in the preceding exercise. Show that $(2x+1)^2 \equiv -3 \bmod p$.

3.27 Let $p \equiv 1 \bmod 4$ be a prime, and let g be a primitive root mod p. Show that, for $x = g^{(p-1)/4}$, we have $x^2 \equiv -1 \bmod p$.

3.28 Let n be an odd integer, and let $p \equiv 1 \bmod n$ be an odd prime. Show that the congruence $x^n \equiv 1 \bmod p$ has a solution $x \not\equiv 1 \bmod p$.

3.29 Here is another way of proving Fermat's First Theorem. Consider the set of all triples xyz with $x, y, z \in \{0, 1\}$. There are clearly 2^3 of them. Now we count them differently:

$$\begin{aligned} &000 \\ &100 + \text{cyclic shifts} \\ &110 + \text{cyclic shifts} \\ &111 \end{aligned}$$

Here the cyclic shifts of 100 are 010 and 001; since there are three cyclic shifts of 100 and three shifts of 110, we must have $2^6 = 2 + 3 \cdot 2$, in other words: $2^3 \equiv 2 \bmod 3$.
Now work out this proof for vectors of length 5 and show that $2^5 \equiv 2 \bmod 5$. Think about what goes wrong for exponent 6, and generalize the proof above to $2^p \equiv 2 \bmod p$. Finally, by letting the entries be from $\mathbb{Z}/p\mathbb{Z}$ instead of $\{0, 1\}$, Fermat's First Theorem follows.

3.30 Let p be a prime number and consider the set

$$\mathbb{Z}[\tfrac{1}{p}] = \{r \in \mathbb{Q} : p^n r \in \mathbb{Z} \text{ for some } n \in \mathbb{N}\}.$$

1. Show that $R = \mathbb{Z}[\frac{1}{p}]$ is a ring.
2. Show that the unit group is generated by -1 and p.
3. Show that the irreducible elements in R are the primes $q \in \mathbb{N}$ with $q \neq p$
4. Show that R is factorial.

3.31 Let $m \geq 2$ be a prime number and consider the set

$$\mathbb{Z}[\tfrac{1}{m}] = \{r \in \mathbb{Q} : m^n r \in \mathbb{Z} \text{ for some } n \in \mathbb{N}\}.$$

1. Show that $R = \mathbb{Z}[\frac{1}{m}]$ is a ring.
2. Show that the unit group is generated by -1 and the prime factors of m.
3. Show that the irreducible elements are the primes $p \in \mathbb{N}$ not dividing m.
4. Show that R is factorial.

3.32 Let p be a prime number and consider the set

$$\mathbb{Z}_{(p)} = \{m \in \mathbb{Q} : nq \in \mathbb{Z} \text{ for some } n \in \mathbb{N} \text{ coprime with } p\}.$$

1. Show that $R = \mathbb{Z}_{(p)}$ is a ring.
2. Show that the unit group is generated by -1 and p.
3. Show that p is the only prime number in R.
4. Show that R is factorial.

3.33 A function $f : \mathbb{N} \longrightarrow \mathbb{C}$ is called a number theoretic function if it is multiplicative in the following sense: $f(mn) = f(m)f(n)$ whenever $\gcd(m,n) = 1$. We have seen that Euler's ϕ function is a number theoretic function. Show that $\sigma(n) = \sum_{d|n} d$, the sum of all divisors of n, is also a number theoretic function.

3.34 In the theory of categories, there is a clear distinction between direct sums and direct products. In this exercise we explain why we have written the direct product of rings as $R \times S$ and not as $R \oplus S$.

In fact, for a direct sum $A \oplus B$ of two groups or rings A and B, we must have homomorphisms $\iota_A : A \longrightarrow A \oplus B$ and $\iota_B : B \longrightarrow A \oplus B$ *into* the direct sum. For direct products, however, we demand that there be projection maps $\pi_A : A \times B \longrightarrow A$ and $\pi_B : A \times B \longrightarrow B$ *from* the direct product to its components.

For groups, constructing maps ι_A and ι_B is easy: set $\iota_A(a) = (a, 0)$ and $\iota_B(b) = (0, b)$, where 0 denotes the neutral elements of A and B. Verify that these are homomorphisms.

For unital rings, this does not work in general: the map ι_A maps the unit element $1 \in A$ to the element $(1, 0)$ in $A \oplus B$, whereas ring homomorphisms of unital rings must map the unit element of A to the unit element $(1, 1)$ of $A \times B$. It can be verified painlessly, however, that the projection maps π_A and π_B defined by $\pi_A((a, b)) = a$ and $\pi_B((a, b)) = b$ are ring homomorphisms.