Example 3.16. *Solve the congruence* $x^2 + x + 47 \equiv 0 \pmod{7^3}$.

Solution: Let us first solve the congruence $x^2 + x + 47 \equiv 0 \pmod 7$. By inserting elements of the complete residue system, we obtain solutions $x \equiv 1 \pmod 7$ and $x \equiv 5 \pmod 7$. Let $f(x) = x^2 + x + 47$. Then $f'(x) = 2x + 1$, so $f'(1) = 3 \not\equiv 0 \pmod 7$ and $f'(5) = 11 \not\equiv 0 \pmod 7$. Therefore, we can apply Hensel's lemma.

To solve the congruence $x^2 + x + 47 \equiv 0 \pmod{7^2}$, we need to solve

$$tf'(a) \equiv -\frac{f(a)}{7} \pmod 7 \quad \text{for } a = 1, 5.$$

We have

1) $t \cdot 3 \equiv -7 \pmod 7 \implies t = 0 \implies a + t \cdot 7 = 1$;
2) $t \cdot 11 \equiv -11 \pmod 7 \implies t = 6 \implies a + t \cdot 7 = 47$.

Finally, to solve the initial congruence, we need to solve

$$tf'(a) \equiv -\frac{f(a)}{49} \pmod 7 \quad \text{for } a = 1, 47.$$

We have:

1) $t \cdot 3 \equiv -1 \pmod 7 \implies t = 2 \implies a + t \cdot 49 = 99$;
2) $t \cdot 11 \equiv -47 \pmod 7 \implies t = 4 \implies a + t \cdot 49 = 243$.

Hence, the solutions are $x \equiv 99 \pmod{343}$ and $x \equiv 243 \pmod{343}$. ♢

3.7 Primitive roots and indices

Definition 3.5. *Let a and n be relatively prime positive integers. The smallest positive integer d such that $a^d \equiv 1 \pmod n$ is called the* order *of a modulo n. It is also said that a* belongs to the exponent *d modulo n.*

Proposition 3.18. *Let d be the order of a modulo n. Then for a positive integer k, $a^k \equiv 1 \pmod n$ if and only if $d \mid k$. In particular, $d \mid \varphi(n)$.*

Proof: If $d \mid k$, say $k = d \cdot l$, then $a^k \equiv (a^d)^l \equiv 1 \pmod n$.

Conversely, assume that $a^k \equiv 1 \pmod n$. By dividing k by d, we obtain $k = q \cdot d + r$, where $0 \le r < d$. Now we have

$$1 \equiv a^k \equiv a^{qd+r} \equiv (a^d)^q \cdot a^r \equiv a^r \pmod n,$$

and from the minimality of d, it follows that $r = 0$, i.e. $d \mid k$. □

Example 3.17. *Prove that all prime divisors of the Fermat number* $2^{2^n}+1$ *have the form* $p = k \cdot 2^{n+1}+1$.

Solution: From $2^{2^n}+1 \equiv 0 \pmod{p}$, it follows that $2^{2^n} \equiv -1 \pmod{p}$ and $2^{2^{n+1}} \equiv 1 \pmod{p}$, so we conclude that 2 belongs to the exponent 2^{n+1} modulo p. Since $\varphi(p) = p-1$, we have $2^{n+1} \mid p-1$. Hence, there is $k \in \mathbb{N}$ such that $p = k \cdot 2^{n+1}+1$.

This result is in line with the fact that the Fermat number $2^{2^5}+1$ is divisible by $641 = 10 \cdot 2^6 + 1$, as we have seen in Chapter 2.3. ♢

Definition 3.6. *If the order of* a *modulo* n *is equal to* $\varphi(n)$*, then* a *is called a* primitive root *modulo* n.

Reduced residues modulo n, with the operation of multiplication modulo n, form a group (the closedness under multiplication and the existence of inverse follow from Theorem 3.8). This group is denoted by $(\mathbb{Z}/n\mathbb{Z})^*$ (or $\mathbb{Z}_n^*$). If there is a primitive root modulo n, then the group $(\mathbb{Z}/n\mathbb{Z})^*$ is cyclic (a primitive root is a generator of the group, every element can be represented as its power). The following theorem shows that the group $(\mathbb{Z}/p\mathbb{Z})^*$, i.e. the multiplicative group of the finite field $\mathbb{F}_p$, is cyclic.

Theorem 3.19. *If* p *is a prime number, then there are exactly* $\varphi(p-1)$ *primitive roots modulo* p.

Proof: Each of the numbers $1, 2, \ldots, p-1$ belongs to some exponent d modulo p, which is a divisor of $\varphi(p) = p-1$. We denote by $\psi(d)$ the number of elements in the sequence $1, 2, \ldots, p-1$ which belong to the exponent d. Then

$$\sum_{d \mid p-1} \psi(d) = p-1.$$

It is sufficient to prove that if $\psi(d) \neq 0$, then $\psi(d) = \varphi(d)$. Indeed, by Theorem 3.12, we have

$$\sum_{d \mid p-1} \varphi(d) = p-1,$$

so if $\psi(d) = 0 < \varphi(d)$ for some d, then the sum $\sum_{d \mid p-1} \psi(d)$ would be less than $p-1$. Hence, $\psi(d) \neq 0$ for every d, so if we show that this implies that $\psi(d) = \varphi(d)$, we will obtain that $\psi(p-1) = \varphi(p-1)$, which is the statement of the theorem.

Let us now prove the statement that $\psi(d) \neq 0$ implies $\psi(d) = \varphi(d)$. Let $\psi(d) \neq 0$ and let a be a number belonging to the exponent d modulo p. Consider the congruence

$$x^d \equiv 1 \pmod{p}.$$

It has solutions $a, a^2, \ldots, a^d$, and by Lagrange's theorem, these are all solutions. Let us show that the numbers a^m, for $1 \leq m \leq d$ and $\gcd(m,d) = 1$, represent all numbers belonging to the exponent d modulo p. Indeed, each of them has order d, because if $a^{md'} \equiv 1 \pmod{p}$, then $d \mid md'$, so $d \mid d'$. If b is any number belonging to the exponent d modulo p, then $b \equiv a^m$ for some m, $1 \leq m \leq d$. Since

$$b^{\frac{d}{\gcd(m,d)}} \equiv (a^d)^{\frac{m}{\gcd(m,d)}} \equiv 1 \pmod{p},$$

we have $\gcd(m,d) = 1$. Hence, we proved that $\psi(d) = \varphi(d)$. □

Theorem 3.20. *Let p be an odd prime number and let g be a primitive root modulo p. Then there exists $x \in \mathbb{Z}$ such that $g' = g + px$ is a primitive root modulo p^j for every $j \in \mathbb{N}$.*

Proof: We have $g^{p-1} = 1 + py$, for some $y \in \mathbb{Z}$. By the binomial theorem, we have

$$(g')^{p-1} = 1 + py + (p-1)pxg^{p-2} + \binom{p-1}{2} p^2x^2g^{p-3} + \cdots + p^{p-1}x^{p-1},$$

i.e. $(g')^{p-1} = 1 + pz$, where $z \equiv y + (p-1)g^{p-2}x \pmod{p}$. The coefficient of x is not divisible by p, so we can choose $x \in \mathbb{Z}$ (in fact $x \in \{0, 1\}$) such that $\gcd(z,p) = 1$. We claim that then g' has the desired property. Let us prove this claim.

Assume that g' belongs to the exponent d modulo p^j. Then d divides $\varphi(p^j) = p^{j-1}(p-1)$. But g' is a primitive root modulo p, so $p-1$ divides d. Hence, $d = p^k(p-1)$ for some $k < j$. Furthermore, we have

$$(1+pz)^p = 1 + p^2z_1, \quad (1+pz)^{p^2} = (1+p^2z_1)^p = 1 + p^3z_2, \ldots,$$
$$(1+pz)^{p^k} = 1 + p^{k+1}z_k,$$

where $\gcd(z_i, p) = 1$ for $i = 1, \ldots, k$. Since $g'^d \equiv 1 \pmod{p^j}$, we conclude that $j = k+1$, which implies that $d = \varphi(p^j)$. □

Theorem 3.21. *Let n be a positive integer. There exists a primitive root modulo n if and only if $n = 1$, 2, 4, p^j, or $2p^j$, where p is an odd prime number.*

Proof: It is clear that 1 is a primitive root modulo 1 and modulo 2, and that 3 is a primitive root modulo 4. Let g be a primitive root modulo p^j. Let us choose among the numbers g and $g + p^j$ the one which is odd. Then it is a primitive root modulo $2p^j$, since $\varphi(2p^j) = \varphi(p^j)$.

It remains to prove the necessity. Let us first consider $n = 2^j$ for $j \geq 3$. For an odd integer a, $a^2 \equiv 1 \pmod 8$. Since $8 \mid a^2 - 1$ and $2 \mid a^2 + 1$, we have $a^4 \equiv 1 \pmod{16}$. By repeating this argument, we obtain $a^{2^{j-2}} \equiv 1 \pmod{2^j}$ for $j \geq 3$. Since $\varphi(2^j) = 2^{j-1}$, we have proved that there does not exist a primitive root modulo 2^j for $j \geq 3$.

Finally, let $n = n_1 n_2$, where $\gcd(n_1, n_2) = 1$, $n_1 > 2$, $n_2 > 2$. The integers $\varphi(n_1)$ and $\varphi(n_2)$ are even, so for a relatively prime to n, we have

$$a^{\frac{1}{2}\varphi(n)} \equiv \left(a^{\varphi(n_1)}\right)^{\frac{1}{2}\varphi(n_2)} \equiv 1 \pmod{n_1},$$
$$a^{\frac{1}{2}\varphi(n)} \equiv \left(a^{\varphi(n_2)}\right)^{\frac{1}{2}\varphi(n_1)} \equiv 1 \pmod{n_2}.$$

Hence $a^{\frac{1}{2}\varphi(n)} \equiv 1 \pmod n$, which means that there is no primitive root modulo n. □

Let us provide some information on methods of determining primitive roots. We can start one by one and test if $g = 2$, $g = 3, \ldots$ is a primitive root. While doing that, the numbers of the form g_0^k, $k \geq 2$ do not need to be tested because if g_0 is not a primitive root, then g_0^k cannot be either. Testing whether g is a primitive root is based on the following fact: g is a primitive root modulo p if and only if for each prime factor q of $p - 1$ we have $g^{(p-1)/q} \not\equiv 1 \pmod p$.

We may ask what is the probability that already $g = 2$ is a primitive root. Concerning this question, let us mention Artin's conjecture which states that for a positive integer a, which is not a power of an integer, $\nu_a(N) \sim A \cdot \pi(N)$, where $\pi(N)$ is the number of primes $\leq N$, $\nu_a(N)$ the number of primes $\leq N$ for which a is a primitive root, while A is Artin's constant

$$\prod_{p \text{ prime}} \left(1 - \frac{1}{p(p-1)}\right) \approx 0.3739558.$$

It is known that the so-called generalized Riemann hypothesis (GRH) implies Artin's conjecture, as well as the estimate $O(\ln^6 p)$ for the least primitive root modulo p (see [93, Chapters 1.6 and 4.5]).

Example 3.18. *Find the least primitive root*

a) modulo 5*,*

b) modulo 11*,*

c) modulo 23*.*

Solution:

a) $2^2 \not\equiv 1 \pmod 5$, so 2 is a primitive root modulo 5.

b) $2^2 \not\equiv 1 \pmod{11}$, $2^5 \not\equiv 1 \pmod{11}$, so 2 is a primitive root modulo 11.

c) $2^{11} = 32 \cdot 64 \equiv 9 \cdot (-5) \equiv 1 \pmod{23}$, so 2 is not a primitive root modulo 23; $3^{11} = 27^3 \cdot 9 \equiv 64 \cdot 9 \equiv (-5) \cdot 9 \equiv 1 \pmod{23}$, so 3 is not a primitive root modulo 23; $5^{11} = (25)^5 \cdot 5 \equiv 32 \cdot 5 \equiv 9 \cdot 5 \equiv -1 \not\equiv 1 \pmod{23}$, $5^2 \equiv 2 \not\equiv 1 \pmod{23}$, so 5 is a primitive root modulo 23. $\diamondsuit$

Let g be a primitive root modulo n. It is easy to see then that the numbers g^l, $l = 0, 1, \ldots, \varphi(n) - 1$ form a reduced residue system modulo n. Indeed, it is sufficient to check that $g^l \not\equiv g^k \pmod n$ for $0 \leq l < k \leq \varphi(n) - 1$. But if $g^l \equiv g^k \pmod n$, then from $g^{k-l} \equiv 1 \pmod n$, we would obtain a contradiction to the assumption that g is a primitive root.

Therefore, for any integer a such that $\gcd(a, n) = 1$ there is a unique $l \in \{0, 1, \ldots, \varphi(n) - 1\}$ such that $g^l \equiv a \pmod n$. The exponent l is called the *index* (or *discrete logarithm*) of a with respect to g and is denoted by $\operatorname{ind}_g a$ or $\operatorname{ind} a$.

Theorem 3.22.

1) $\operatorname{ind} a + \operatorname{ind} b \equiv \operatorname{ind}(ab) \pmod{\varphi(n)}$*;*

2) $\operatorname{ind} 1 = 0, \quad \operatorname{ind}_g g = 1$*;*

3) $\operatorname{ind}(a^m) \equiv m \operatorname{ind} a \pmod{\varphi(n)}$ *for* $m \in \mathbb{N}$*;*

4) $\operatorname{ind}(-1) = \frac{1}{2}\varphi(n)$ *for* $n \geq 3$*.*

Proof: Properties 1) – 3) follow directly from the definition of index and properties of multiplication and exponentiation of powers, while property 4) follows from $g^{2\operatorname{ind}(-1)} \equiv (-1)^2 \equiv 1 \pmod n$ and $2\operatorname{ind}(-1) < 2\varphi(n)$. $\square$

Let us note that properties 1) – 3) of the index are analogous to the properties of the logarithmic function. Note also that when "indexing" a congruence, the modulus changes and we get the modulus $\varphi(n)$, instead of n.

Proposition 3.23. *If* $\gcd(n, p-1) = 1$*, then the congruence* $x^n \equiv a \pmod{p}$ *has a unique solution.*

Proof: From $x^n \equiv a \pmod{p}$, by Theorem 3.22, we obtain

$$n \operatorname{ind} x \equiv \operatorname{ind} a \pmod{p-1},$$

so since $\gcd(n, p-1) = 1$, this congruence has a unique solution. □

Example 3.19. *Solve the congruence* $x^5 \equiv 2 \pmod{7}$.

Solution: We have $3^2 \equiv 2 \pmod{7}$, $3^3 \equiv 6 \pmod{7}$, $3^6 \equiv 1 \pmod{7}$. Hence, 3 is a primitive root modulo 7 and $\operatorname{ind}_3 2 = 2$. Thus, we obtain the congruence

$$5 \operatorname{ind}_3 x \equiv 2 \pmod{6},$$

whose solution is $\operatorname{ind}_3 x = 4$, so $x \equiv 3^4 \equiv 4 \pmod{7}$. ♢

Example 3.20. *Solve the congruence* $5x^4 \equiv 3 \pmod{11}$.

Solution: From Example 3.18, we know that 2 is a primitive root modulo 11. Furthermore, $2^4 \equiv 5 \pmod{11}$ and $2^8 \equiv 3 \pmod{11}$, so we obtain

$$\operatorname{ind}_2 5 + 4 \operatorname{ind}_2 x \equiv \operatorname{ind}_2 3 \pmod{10}, \quad 4 \operatorname{ind}_2 x \equiv 8 - 4 \equiv 4 \pmod{10}.$$

Accordingly, we need to solve the congruence $2 \operatorname{ind}_2 x \equiv 2 \pmod{5}$. From this, we get $\operatorname{ind}_2 x \equiv 1$ or $6 \pmod{10}$, and the solutions are $x \equiv 2 \pmod{11}$ and $x \equiv 2^6 \equiv 9 \pmod{11}$. ♢

Example 3.21. *Solve the congruence* $3^x \equiv 2 \pmod{23}$.

Solution: From Example 3.18, we know that 5 is a primitive root modulo 23. Furthermore, $5^2 \equiv 2 \pmod{23}$, $5^5 \equiv 2^2 \cdot 5 \equiv -3 \pmod{23}$, $5^{11} \equiv -1 \pmod{23}$, which gives $5^{16} \equiv 3 \pmod{23}$. We have

$$x \operatorname{ind}_5 3 \equiv \operatorname{ind}_5 2 \pmod{22}, \quad 16x \equiv 2 \pmod{22}.$$

Now $\gcd(16, 22) = 2$, so we obtain $8x \equiv 1 \pmod{11}$, which implies $x \equiv 7 \pmod{11}$. Thus, the solutions are $x \equiv 7, 18 \pmod{22}$. ♢

When the modulus n is small, we can calculate indices by creating a table of all values $g^l \bmod n$ for $l = 0, 1, \ldots, \varphi(n)-1$ (while doing so, it is sufficient to calculate values for l up to $\varphi(n)/2$ and apply Theorem 3.22.4)). For larger moduli n, more efficient methods for calculating the discrete logarithm can be used (for example, the *index calculus* method, on which we will provide more information in Chapter 15.8).

Example 3.22. *Let $\alpha \geq 3$. Prove that the numbers*

$$\pm 5,\ \pm 5^2,\ \pm 5^3, \ldots,\ \pm 5^{2^{\alpha-2}}$$

form a reduced residue system modulo 2^α.

Solution: There are $2 \cdot 2^{\alpha-2} = 2^{\alpha-1} = \varphi(2^\alpha)$ numbers in the list, and they are all odd. Therefore, we only need to prove that they are incongruent modulo 2^α.

Let us show that for $k \geq 2$, $2^k \parallel (5^{2^{k-2}} - 1)$. The claim is true for $k = 2$, so we assume that it holds for some k. Then

$$5^{2^{k-1}} - 1 = \left(5^{2^{k-2}} - 1\right)\left(5^{2k-2} + 1\right).$$

The number $5^{2^{k-2}} + 1$ is even, but it is not divisible by 4, so $2^{k+1} \parallel \left(5^{2^{k-1}} - 1\right)$.

By inserting $k = \alpha$ in the statement just proved, we conclude that the order of 5 modulo 2^α is equal to $2^{\alpha-2}$. This means that the numbers $5,\ 5^2, \ldots,\ 5^{2^{\alpha-2}}$ are incongruent modulo 2^α. It remains to check that we cannot have $5^a \equiv -5^b \pmod{2^\alpha}$, but this is obvious since $5^a + 5^b \equiv 2 \pmod 4$. ♢

3.8 Representations of rational numbers by decimals

A well-known property of rational numbers is that their decimal representation is either finite or eventually periodic (periodic from some point onwards; we will often just say periodic, while the representations without pre-period will be called purely periodic). For example, $\frac{3}{8} = 0.375$, $\frac{7}{15} = 0.4666\cdots = 0.4\dot{6}$, $\frac{1}{7} = 0.142857142857\cdots = 0.\dot{1}42857\dot{}$. In this section, we will show that this property characterizes rational numbers, and we will consider some properties of rational numbers with periodic decimal representation. We will see that the length of the period of these numbers is connected to the question of number 10 being a primitive root modulo the denominator of the rational number, and what is the order of 10 modulo that denominator. Among the number theory books dealing with this topic, let us mention [211, 254, 330, 369, 383].

In these considerations, the integer part of a rational number p/q is usually ignored because it does not impact the finiteness nor the periodicity of decimal representation. Therefore, we will assume that $0 < p < q$ and $\gcd(p, q) = 1$.

Proposition 3.24. *The decimal representation of a rational number $r = p/q$ is finite if and only if the denominator q contains only 2 and 5 as prime factors.*