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

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

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

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.*

Proof: Let $\frac{p}{q} = 0.a_1a_2\cdots a_n = \frac{a_1}{10} + \frac{a_2}{10^2} + \cdots + \frac{a_n}{10^n}$. Then from

$$\frac{p}{q} = \frac{a_1 10^{n-1} + a_2 10^{n-2} + \cdots + a_n}{10^n}$$

we conclude that q divides 10^n. Hence, q contains only prime factors 2 and 5.

Assume now that $q = 2^\alpha 5^\beta$; namely, that a rational number r has the form $r = \frac{p}{2^\alpha 5^\beta}$. Let $\alpha \geq \beta$ (we proceed analogously if $\alpha < \beta$). By multiplying the numerator and denominator by $5^{\alpha-\beta}$, we obtain $r = \frac{5^{\alpha-\beta}p}{10^\alpha}$, which shows that the decimal representation of the number r is finite. From the proof, it also follows that the number of decimal digits in the representation of r is $\max(\alpha, \beta)$. □

Finite decimal representation can be understood as a special case of (eventually) periodic representation in which the digit 0 (or the digit 9) repeats indefinitely. For example, $3/8 = 0.375 = 0.375\dot{0} = 0.374\dot{9}$.

Theorem 3.25. *A real number r is rational if and only if its decimal representation is finite or eventually periodic.*

Proof: If r has a finite decimal representation, then it is equal to a sum of finitely many rational numbers, so it is evidently a rational number. Assume that r has a periodic decimal representation. Let t be the length of the period and let the repetition start after s decimals (the pre-period is of length s). We have

$$r = 0.a_1a_2\cdots a_s b_1b_2\cdots b_t b_1b_2\cdots b_t\cdots . \tag{3.5}$$

Let us multiply the left and right-hand side of (3.5), first by 10^{s+t}, and then by 10^s. We obtain

$$\begin{aligned} 10^{s+t}r &= a_1a_2\cdots a_s b_1b_2\cdots b_t\,.\,b_1b_2\cdots b_t b_1b_2\cdots b_t\cdots , \\ 10^s r &= a_1a_2\cdots a_s\,.\,b_1b_2\cdots b_t b_1b_2\cdots b_t\cdots . \end{aligned}$$

The two obtained numbers coincide in the decimal representation after the decimal point (it is said that they have identical *mantissa*), meaning that their difference is an integer. Let us denote that difference by c. By subtraction, we obtain

$$r = \frac{c}{10^{s+t} - 10^s},$$

which implies that r is a rational number.

Let us prove the converse. Let $r = p/q$ be a rational number. Consider the sequence of rational numbers

$$\frac{p}{q}, \frac{10p}{q}, \frac{10^2p}{q}, \frac{10^3p}{q}, \dots$$

Their numerators $p, 10p, 10^2p, 10^3p, \dots$ cannot all have different remainders in the division by q, because there are infinitely many numerators, but only finitely many possible remainders. Therefore, there are integers $s \geq 0$ and $t \geq 1$ such that

$$10^s p \equiv 10^{s+t} p \pmod{q}. \tag{3.6}$$

The two corresponding rational numbers $\frac{10^s p}{q}$ and $\frac{10^{s+t} p}{q}$ differ by an integer, so they have identical mantissas. Therefore, if we delete the first s decimals or the first $s+t$ decimals from the mantissa of p/q, we will obtain the same number. This means that the decimal representation of p/q is periodic. More precisely, the repetition begins after s decimals, and the length of the period (group of decimals which repeats) is t. □

The following statement follows directly from the proof of Theorem 3.25.

Corollary 3.26. *Let $r = p/q$ be a rational number. If t is the length of the shortest period of its decimal representation, and the repetition begins after s decimals, then s and t are the smallest integers satisfying $s \geq 0$, $t \geq 1$ and*

$$10^{s+t} \equiv 10^s \pmod{q}. \tag{3.7}$$

From Corollary 3.26, we notice an interesting fact that the lengths of period and pre-period in the decimal representation of a rational number p/q do not depend on its numerator p, but only on its denominator q.

We can ask when will the decimal representation of a rational number p/q be purely periodic, i.e. will not have a non-repeating part. The condition that there is no pre-period means that $s = 0$. If $\gcd(10, q) = 1$, then from (3.7), it follows that $10^t \equiv 1 \pmod{q}$, so the least non-negative integer for which (3.7) holds is exactly $s = 0$, while the period t is equal to the order of 10 modulo q. The converse also holds. If $s = 0$, then $10^t \equiv 1 \pmod{q}$, so $\gcd(10, q) = 1$. Thus, we have proved the following characterization of rational numbers with purely periodic decimal representation.

Corollary 3.27. *The decimal representation of a rational number $r = p/q$ is purely periodic (without pre-period) if and only if the denominator q is not divisible by 2 or by 5, while the length of the period is equal to the order of 10 modulo q.*

From Corollary 3.27 and Proposition 3.18, it follows that for a rational number p/q with purely periodic decimal representation, the period t divides $\varphi(q)$. From what we already proved, the following general result follows.

Corollary 3.28. *If the denominator of a rational number p/q has the form $q = 2^\alpha 5^\beta q_0$, where $\gcd(10, q_0) = 1$, then the decimal representation of p/q contains a pre-period of length $\max(\alpha, \beta)$, and the length of the period is equal to the order of 10 modulo q_0.*

Example 3.23. Consider the number $33/260$. Since $260 = 2^2 \cdot 5 \cdot 13$, by Corollary 3.28, its decimal representation should contain a pre-period of length 2 and a period of the length equal to the order of 10 modulo 13, and that is 6. Indeed,

$$\frac{33}{260} = 0.12\dot{6}92307\dot{}. \qquad \diamondsuit$$

For period t in the decimal representation of p/q, where $q = 2^\alpha 5^\beta q_0$, we have $t \le \varphi(q_0) \le \varphi(q) \le q - 1$. The equality $t = q - 1$ holds if and only if q is a prime and 10 is a primitive root modulo q. By the previously mentioned Artin's conjecture, there should be infinitely many primes with this property. For example, such numbers are:

$$7, 17, 19, 23, 29, 47, 59, 61, 97, 109, 113, 131, 149, 167, 179, 181, 193, \ldots$$

Example 3.24. Let us check that rational numbers with denominators 7, 17, 19 and 23 have the maximal period:

$$\begin{aligned}
\frac{1}{7} &= 0.\dot{1}42857\dot{}, \\
\frac{1}{17} &= 0.\dot{0}588235294117647\dot{}, \\
\frac{1}{19} &= 0.\dot{0}52631578947368421\dot{}, \\
\frac{1}{23} &= 0.\dot{0}434782608695652173913\dot{}. \qquad \diamondsuit
\end{aligned}$$

Consider the decimal representation of $1/19$ from Example 3.24. The length of its period is 18. Let us split the mantissa into two parts of length 9 and add the two parts:

$$052631578 + 947368421 = 999999999.$$

Let us now choose a rational number with a prime denominator which does not have the maximal length of the period (but such that the length of the period is even, so that the previous process makes sense), for example, $9/13 = 0.\dot{6}92307\dot{}$. We obtain $692 + 307 = 999$. The fact that lies behind these examples is called Midy's theorem.

Theorem 3.29 (Midy, 1836)**.** *Let $q \neq 2, 5$ be a prime number and let $0 < p < q$. If*

$$\frac{p}{q} = 0.\dot{b_1}b_2 \cdots \dot{b_t}$$

is the decimal representation of p/q and if the length of the period t is even, say $t = 2u$, then

$$\overline{b_1 b_2 \cdots b_u} + \overline{b_{u+1} b_{u+2} \cdots b_{2u}} = \underbrace{999\ldots9}_{u \text{ nines}}.$$

Proof: Let $A = \overline{b_1 b_2 \cdots b_u} = b_1 10^{u-1} + b_2 10^{u-2} + \cdots + b_u$ and $B = \overline{b_{u+1} b_{u+2} \cdots b_{2u}} = b_{u+1} 10^{u-1} + b_{u+2} 10^{u-2} + \cdots + b_{2u}$. Then

$$\begin{aligned} \frac{p}{q} &= \frac{A}{10^u} + \frac{B}{10^{2u}} + \frac{A}{10^{3u}} + \frac{B}{10^{4u}} + \cdots \\ &= (10^u A + B)\Big(\frac{1}{10^{2u}} + \frac{1}{10^{4u}} + \cdots\Big) \\ &= \frac{10^u A + B}{10^{2u} - 1} \end{aligned}$$

(by the formula for the sum of a geometric series). Hence,

$$p(10^u - 1)(10^u + 1) = q(10^u A + B). \tag{3.8}$$

From (3.8), it follows that $q \mid (10^u - 1)$ or $q \mid (10^u + 1)$. If $q \mid (10^u - 1)$, then the order of 10 modulo q is $\leq u < 2u$, and we obtain a contradiction. Therefore, we conclude that $q \mid (10^u + 1)$. Now, from (3.8), it follows that $10^u - 1$ divides $10^u A + B$, i.e.

$$A + B \equiv 0 \pmod{10^u - 1}. \tag{3.9}$$

On the other side, we have $0 \leq A, B \leq 10^u - 1$. The numbers A and B cannot both be equal to 0 because $p > 0$ and $A + B > 0$. Also, the numbers A and B cannot both be equal to $10^u - 1$ because this would mean that $p/q = 0.999\cdots = 1$, which contradicts the assumption that $p < q$. Therefore, we have

$$0 < A + B < 2(10^u - 1),$$

which, together with (3.9), gives

$$A + B = 10^u - 1 = 999 \cdots 9. \qquad \square$$

In this section, we considered properties of representations of rational numbers with the basis 10. Similar matters can be considered for representation with an arbitrary basis b. The role of the numbers 2 and 5 in results of this section is then replaced by prime factors of b. For details, consult [211, Chapter 9.3].

3.9 Pseudoprimes

In various applications of number theory, especially in applications in public-key cryptography on which we will focus further on in the book, the first step is choosing one or more large prime numbers. In the RSA cryptosystem, by using large private (secret) prime numbers p and q, we create public modulus n. On the other hand, in ElGamal's cryptosystem, a large public prime number p determines the corresponding finite field $\mathbb{F}_p$ in which encryption takes place. The role of primes in these two cryptosystems is not quite the same. In the case of ElGamal's cryptosystem, where p is a public value, we are allowed to use for p a number recommended in the literature. On the other hand, for the security of the RSA cryptosystem, it is necessary that the numbers p and q are confidential.

We see that in the public-key cryptography, an important question is how to determine whether a given positive integer is prime or composite. In this section, we will say something about the so-called primality tests. These are the criteria that a number p must satisfy to be prime. So if p does not meet any of these criteria, then it is certainly composite, and if it satisfies them, then it is "probably prime", which means that it is very likely that p is prime. Later on, in Chapter 15.9, we will show some of the methods used for rigorously proving that a number is prime. However, in applications, it is often satisfactory to find numbers that are very likely to be prime. It is important to mention that these tests are much faster than all known methods for proving primality.

The reason for the distinction between testing and proving primality lies in the fact that properties that completely characterize prime numbers (like Wilson's theorem) are not easy to check. On the other hand, some important properties of prime numbers are very easy to verify; however, they do not characterize prime numbers, i.e. there are also some composite numbers