## Contents

Chapter 1. Primes  
1.1. The elementary operations 3  
1.2. Even and odd 4  
1.3. Prime numbers 5  
1.4. The set of primes 6  
1.5. Diophantine equations 7  
1.6. gcd and lcm 8  
1.7. The fundamental theorem of arithmetic 9  

Chapter 2. Congruences 11  
2.1. Gauss’ notation for congruences 11  
2.2. Applications 12  
2.3. Arithmetic properties 13  
2.4. Fermat and Euler theorems 14
These are notes prepared for the course *Theory of Numbers*, taught at Rutgers in Spring 2019. We follow the organization of Davenport’s *Higher Arithmetic* (Cambridge University Press, 8th Ed.) with some additional supplements.

[…] the subject matter is so attractive that only extravagant incompetence could make it dull.

– G.H. Hardy, E.M. Wright, *Introduction to the Theory of Numbers*
1.1. The elementary operations

Arithmetic (from the Greek, \textit{arithmos}, number, \textit{tike}, art) is the study of numbers and their properties under the elementary operations of adding, subtracting, multiplying, and dividing.

The set of (natural) numbers\footnote{Here, we will work in the French tradition of considering 0 as a number.} is

\[ \mathbb{N} = \{0, 1, 2, \ldots\} . \]

This set is infinite countable, and totally ordered (i.e. for any two elements \(a, b \in \mathbb{N}\), either \(a \leq b\) or \(b \leq a\)). We take for granted the following ‘laws of arithmetic’: for any \(a, b, c \in \mathbb{N}\),

(1) addition and multiplication are commutative: \(a + b = b + a\), \(ab = ba\),

(2) addition and multiplication are associative: \(a + (b + c) = (a + b) + c\), \(a(bc) = (ab)c\),

(3) multiplication is distributive with respect to addition: \(a(b + c) = ab + ac\).

If \(a, b \in \mathbb{N}\), then \(a - b \in \mathbb{N}\) if and only if \(a - b \geq 0\). That is, \(\mathbb{N}\) is not closed under subtraction (\(1 - 2 = -1 \not\in \mathbb{N}\)). For this, we have the ring of integers

\[ \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} . \]

Similarly, \(\frac{a}{b} \in \mathbb{N}\) if and only if \(a\) is a multiple of \(b\). For this, we have the field of fractions

\[ \mathbb{Q} = \{\frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{N}\} . \]

We won’t introduce here the algebraic terminology of rings and fields. Just think that a ring is a set closed under addition, multiplication, and subtraction, such that each element has an additive inverse \(a + (-a) = 0\), while a field is a set closed under all four operations, and such that each element has an additive and a multiplicative inverse \(a \cdot a^{-1} = 1\). Other examples of fields are \(\mathbb{R}\) and \(\mathbb{C}\). These are successively larger than \(\mathbb{Q}\) as \(\mathbb{R}\) is also closed under taking the square root of positive integers, and \(\mathbb{C}\) is closed under taking all square roots (since \(\sqrt{-1} \in \mathbb{C}\)).

We write \(a \mid b\) to say \(a\) divides \(b\).

**Example 1.** \(1, 2, 3, 4, 6, 12, 18, 36 \mid 36, 5 \nmid 36\).

Note that if \(a, b \in \mathbb{N}\) and \(a \mid b\), there exists \(n \in \mathbb{N}\) such that \(b = an\). If \(a, b \in \mathbb{Z}\) and \(a \mid b\), there exists \(n \in \mathbb{Z}\) such that \(b = an\).
Proposition 2. Take note of the following basic properties of division.

(1) If \(a|b, b \neq 0\), then \(a \leq b\)

(2) If \(a|b\) and \(b|c\) then \(a|c\)

(3) If \(a|b\) and \(a|c\), then for any \(u, v \in \mathbb{Z}\), \(a|ub + vc\).

Proof. (1) Since \(b = an\) for \(n \geq 1, b \geq a\).

(2) If \(b = an, c = bm\), then \(c = (an)m = a(nm)\), i.e. \(a|c\).

(3) If \(b = an, c = am\), then for any \(u, v \in \mathbb{Z}\),
\[ub + vc = u(an) + v(am) = a(un + vm)\].

1.2. Even and odd

Definition 3. We say that \(n\) is even if \(2|n\) and odd otherwise.

In particular, any even number is of the form \(2k\) (for some \(k \in \mathbb{N}\)) and any odd number is of the form \(2k + 1\). E.g. \(3 = 2 + 1, 17 = 2 \cdot 8 + 1, 14 = 2 \cdot 7\). Of course, \(k\) is then itself either even or odd... Here are some warm-up exercises.

Proposition 4. Any odd number is either of the form \(4k + 1\) or \(4k - 1\).

Proof. Let \(n = 2k + 1\). Then \(k\) is either odd, \(k = 2j - 1\), or even \(k = 2j\). Hence either \(n = 4j - 1\) or \(n = 4j + 1\).

Proposition 5. If \(n \in \mathbb{N}\) is odd, then \(n^2\) is odd.

Proof. Since \(n\) is odd, \(n = 2k + 1\) for some \(k \in \mathbb{N}\). Then
\[n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1\].

Proposition 6. The sum of the first \(n\) odd numbers is \(n^2\).

Proof. The statement is formalized by the equation
\[\sum_{k=0}^{n-1} (2k + 1) = n^2\]
1.3. PRIME NUMBERS

and easily proven by induction. First, it clearly holds for $n = 1$. Assume it is true for $n$. Then
\[
\sum_{k=0}^{n} (2k + 1) = \sum_{k=0}^{n-1} (2k + 1) + 2n + 1 = n^2 + 2n + 1 = (n + 1)^2.
\]

\[\square\]

1.3. Prime numbers

Any $n \in \mathbb{N}$ has at least two divisors: 1 and itself. We refer to those as the trivial divisors of $n$.

Definition 7. If $n \geq 2$ is only divisible by 1 and $n$, it is **prime**. Otherwise we say that $n$ is **composite**.

In particular, if $n$ is composite, there exist $1 < u, v < n$ such that $n = uv$.

Theorem 2. Any $n \geq 2$ is either prime or factorizes as a product of primes, i.e.
\[
n = p_1 \cdots p_k.
\]

Proof. Suppose that the statement is true up to $n - 1$. Suppose further that $n$ is composite. There exist $1 < u, v < n$ such that $n = uv$. By our induction hypothesis, both $u$ and $v$ factor into a product of primes: $u = p_1 \cdots p_j$, $v = q_1 \cdots q_l$. Hence $n = uv = p_1 \cdots q_l$ also factorizes as a product of primes. \[\square\]

Example 8. $1000 = 2^3 \cdot 5^3$, $999 = 3 \cdot 37$.

The prime factorization of any number is unique (up to rearrangements); this is called the fundamental theorem of arithmetic. We will prove this soon.

Example 9. Here are all the primes below 100:
\[
\]

How do we check that a given number is prime? Is there a smarter way to proceed than just by brute force, i.e. checking that no smaller number is a divisor? For the moment, we only record the following observation.

Theorem 3. If $n$ has no prime divisors $\leq \sqrt{n}$ then $n$ is prime.

Proof. Suppose for contradiction that $n$ is composite. In particular, $n$ has at least two distinct prime factors $p$, $q$ and there is an $m \geq 1$ such that $n = pqm$. By assumption, $p, q > \sqrt{n}$, hence $n > nm \geq n$, which is absurd. \[\square\]

Example 10. Since $2, 3, 5 \nmid 37$, it is prime.

Another question is whether we can determine efficiently the prime factorization of a given large number. Here we present a trick of Fermat for factorizing using the ‘difference of squares.’ Suppose you are given $n \in \mathbb{N}$. Pick the smallest number $a$ such that $a^2 > n$. At some point in the sequence
\[
a^2 - n, (a + 1)^2 - n, (a + 2)^2 - n, \ldots
\]
there is a perfect square \( b^2 \), i.e. for some \( k \in \mathbb{N} \), \( (a + k)^2 - n = b^2 \), or equivalently
\[
n = (a + k - b)(a + k + b).
\]
Let’s now see a numerical example. Let \( n = 10'001 \). It is easy to see that \( 100^2 = 10'000 < n < 101^2 \). Hence \( a = 101 \). Now we can quickly compute
\[
101^2 - n = 200, 102^2 - n = 403, \ldots, 105^2 - n = 1024 = 32^2
\]
leading to the factorization \( 10'001 = (105 - 32)(105 + 32) = 73 \cdot 137 \). These factors are small enough that we can very quickly check that 73 and 137 are both primes.

### 1.4. The set of primes

**Theorem 4 (Euclid).** There are infinitely many primes.

**Proof.** Suppose for contradiction that there are only finitely many primes: \( 2, 3, 5, \ldots, p \). Consider
\[
N = 2 \cdot 3 \cdots p + 1.
\]
By assumption, \( N \) is not prime since \( N > p \). Since it is odd, it must have an odd prime factor \( q | N \). Then \( q \) is an element of our finite list of primes \( 2, 3, \ldots, p \). In particular, \( q | (2 \cdot 3 \cdots p) \), hence
\[
q | (N - 2 \cdot 3 \cdots p) = 1,
\]
which is absurd. \( \Box \)

Now that we know that the set of primes is infinite, we may want to know how it is distributed in \( \mathbb{N} \). This is not well understood, and relates to the famous (yet unproven) Riemann hypothesis. Let us explore a first question in this direction. Apart from 2, all prime numbers are odd. Now, we have seen that an odd number is either of the form \( 4k + 1 \) or of the form \( 4k - 1 \). Are there infinitely many primes of both forms?

**Theorem 5.** There are infinitely many primes of the form \( 4k - 1 \).

**Proof.** We mimic Euclid’s argument: suppose that there are only finitely many primes of the form \( 4k - 1 \): \( 3, 7, 11, \ldots, p \), and consider
\[
N = 4(3 \cdot 7 \cdots p) - 1.
\]
By assumption \( N \) is not prime and odd. We show that not all prime divisors of \( N \) can be of the form \( 4k + 1 \). In fact, since
\[
(4k + 1)(4l + 1) = 4(4kl + k + l) + 1,
\]
if all prime divisors of \( N \) were of the form \( 4k + 1 \), then \( N \) would also be of the form \( 4k + 1 \). Hence \( N \) has a prime divisor \( q \) of the form \( 4k - 1 \). Hence \( q | (3 \cdot 7 \cdots p) \) also and \( q | (3 \cdot 7 \cdots p - N) = 1 \), which is absurd. \( \Box \)

Remark that the same argument can not be used to prove that there are infinitely many primes of the form \( 4k + 1 \) (why?). This is nonetheless also true, as we will see later. Actually, a much stronger result is known; this is Dirichlet’s theorem on arithmetic progressions.
Theorem 6 (Dirichlet). Any arithmetic progressions contains infinitely many primes. In other words, there are infinitely many primes of the form \( ax + b \).

The proof of Dirichlet’s theorem is unfortunately outside of the scope of this course, but should be studied by anyone who wants to delve deeper in number theory!

1.5. Diophantine equations

If we know that every arithmetic progressions contains infinitely many primes, we can think of a more general question: given a polynomial \( f(x) = a_n x^n + \cdots + a_1 x + a_0 \) with integer coefficients \( a_0, a_1, \ldots, a_n \in \mathbb{Z} \), are there infinitely many primes in its image \( f(\mathbb{Z}) \)? Well, currently, as soon as \( n > 1 \), nothing is known! A reasonable guess is that things would be easier if we have instead a polynomial with several variables, \( f(x_1, x_2, \ldots, x_n) \).

A Diophantine equation is a polynomial equation with at least two unknowns. For example:

**Example 11.**

1. \( ax + by = c \). In general, a polynomial equation where all terms have degree 1 is called a linear Diophantine equation.

2. \( x^2 + y^2 = z^2 \). The integer solutions to this equation are called Pythagorean triples and have been completely described by Euclid.

3. \( x^n + y^n = z^n \), for \( n \geq 3 \). **Fermat’s last theorem** (proven by Wiles in 1994) states that these have no integer solutions.

4. \( x^2 - ny^2 = 1 \), \( (n \neq k^2) \), is called Pell’s equation.

Cracking a nut with a sledgehammer:

**Theorem 7.** \( \sqrt{2} \) is irrational for \( n \geq 3 \).

**Proof.** Suppose for contradiction that \( \sqrt{2} = \frac{a}{b} \). This is equivalent to \( 2b^2 = a^2 + b^2 = a^n \), which contradicts Fermat’s last theorem. \( \square \)

**Definition 12.** We say that \( a, b \in \mathbb{N} \) are coprime if they have no common prime factor.

**Example 13.** \( 15 = 3 \cdot 5 \) and \( 4 = 2 \cdot 2 \) are coprime.

**Theorem 8.** If \( a, b \in \mathbb{N} \) are coprime, then the linear Diophantine equation

\[
ax + by = c
\]

has integer solutions.

**Proof.** Let \( d \geq 1 \) be the smallest positive number of the form \( ax + by \):

\[
d = ax_0 + by_0.
\]

We will show that \( d|a \) and \( d|b \). Since \( a \) and \( b \) are coprime, we must have \( d = 1 \). Then \( a(x_0c) + b(y_0c) = c \) is a solution. To show that \( d|a \), we divide \( a \) by \( d \): there are two numbers \( q, r \) such that \( a = qd + r \) and \( 0 \leq r < d \). Then

\[
r = a - qd = a - q(ax_0 + by_0) = a(1 - qx_0) + b(-qy_0)
\]

is either 0 or contradicts the minimality of \( d \). This proves that \( d|a \). We can make the exact same argument to prove \( d|b \). \( \square \)
A moment of consideration should convince you that there are solvable equations \( ax + by = c \) where \( a \) and \( b \) are not coprime; for example, \( 2x + 4y = 6 \). You will also notice in this example that all coefficients have 2 as a common divisor.

### 1.6. gcd and lcm

**Definition 14** (gcd). Let \( a, b \in \mathbb{Z} \). The greatest common divisor of \( a \) and \( b \) is the positive integer \( d \) such that

1. \( d \mid a \) and \( d \mid b \) and
2. for any other common divisor \( c \) of \( a \) and \( b \), \( c \leq d \). The shorthand notation for the gcd is \( d = (a, b) \).

**Theorem 9.** The linear Diophantine equation \( ax + by = c \) has integer solutions if and only if \( (a, b) \mid c \).

**Proof.** Choose \( d \) as previously; let it be the smallest positive number of the form \( ax + by \). Then we have seen that \( d \mid a \) and \( d \mid b \). Moreover, for any \( m \) such that \( m \mid a \), \( m \mid b \), then \( m \mid ax + by = d \). Hence \( d = (a, b) \).

If \( d \mid c \), there is a \( k \) such that \( c = dk \), and \( a(xk) + b(yk) = dk = c \) is an example of solution. Conversely, if \( ax + by = c \), we have that \( d \mid c \) since \( d \mid a \) and \( d \mid b \). \( \square \)

A very useful representation of the gcd for practical manipulations is given by the following corollary.

**Corollary 15** (Bézout’s Lemma). For any \( a, b \in \mathbb{Z} \), there exist \( u, v \in \mathbb{Z} \) such that \( au + bv = (a, b) \).

**Exercise 16.** Use Bézout’s lemma to show that if \( c 
mid a \) and \( c 
mid b \), then \( c \mid (a, b) \).

To compute the gcd of two numbers one can rely on their unique prime factorization or on the Euclidean division algorithm.

**Example 17.** \((36, 45) = (2^2 \cdot 3^2, 3^2 \cdot 5) = 3^2 = 9, (422, 7\cdot491) = (2\cdot211, 3\cdot11\cdot227) = 1 \). 

**Theorem 10.** The gcd \((a, b)\) is the last nonzero remainder when running the division algorithm.

**Proof.** We may assume that \( a \geq b \). by the division algorithm, \( a = bq + c \) with \( 0 \leq c < b \). If \( d \mid a \) and \( d \mid b \), then \( d \mid r = a - bq \). Conversely if \( d \mid r \) and \( d \mid b \) then \( d \mid a \). Hence \((a, b) = (b, c)\). Repeating this process a finite number of time, we have

\[
(a, b) = (b, c) = \cdots = (l, m) = (m, n)
\]

with \( l = q'm + n, 0 \leq n < m, \) and \( m = q''n \). Hence \((a, b) = (m, n) = n \). \( \square \)

**Example 18.** \( 7491 = 17 \cdot 422 + 317 \rightarrow 422 = 317 + 105 \rightarrow 317 = 3 \cdot 105 + 2 \rightarrow 105 = 52 \cdot 2 + 1 \).

**Definition 19.** The least common multiplier \( \{a, b\} \) is the number such that

1. \( a \mid \{a, b\} \) and \( b \mid \{a, b\} \), and
2. for any other common multiple \( a \mid c, b \mid c \), \( \{a, b\} \leq c \).

**Theorem 11.** \( ab = \{a, b\}(a, b) \).
1.7. The fundamental theorem of arithmetic

Theorem 12 (Euclid’s lemma). If \( a, b \) are coprime and \( a \mid bc \), then \( a \mid c \).

Proof. By Bézout’s lemma, there exist \( u, v \in \mathbb{Z} \) such that \( au + bv = 1 \). Multiplying both sides by \( c \) yields

\[
auc + bcv = auc + anv = a(uc +nv) = c.
\]

Euclid’s lemma is actually equivalent to the fundamental theorem of arithmetic. In fact, we will prove the latter using Euclid’s lemma in the next section, but we can also prove Euclid’s lemma with the fundamental theorem of arithmetic:

Proof of Euclid’s lemma using the fund. thm. of arithmetic. Consider the prime factorizations \( b = p_1 \cdots p_k, c = q_1 \cdots q_l \). Since \( a \) and \( b \) have no common prime factors, none of \( p_1, \ldots, p_k \) appear in the prime factorization of \( a \). Hence \( a \mid c \).

Two neat consequences of Euclid’s lemma.

Theorem 13. Let \((x_0, y_0)\) be a solution of the linear Diophantine equation \(ax + by = 1\) with \(a, b \) coprime. Then the set of all solutions to \(ax + by = 1\) is

\[
\{(x, y) : x = x_0 - bn, \ y = y_0 + an, \ n \in \mathbb{Z} \}.
\]

Proof. If \((x_0, y_0)\) is a solution, then

\[
a(x_0 - bn) + b(y_0 + an) = ax_0 + by_0 = 1
\]

for each \(n \in \mathbb{Z}\). Conversely, suppose that \(ax + by = 1\). Then subtracting this equation to \(ax_0 + by_0 = 1\), we have

\[
a(x_0 - x) + b(y_0 - y) = 1 - 1 = 0,
\]

hence \(a|b(y - y_0)\) and by Euclid’s lemma, \(a|(y - y_0)\). Say \(y - y_0 = an\). Then

\[
a(x_0 - x) - ban = 0
\]

and \(x = x_0 - bn\).

Theorem 14. A number \(n \geq 2\) is prime if and only if \(n|ab\) implies that \(n|a\) or \(n|b\).
PROOF. Suppose that \( n = p \) is prime. Then the claim follows directly by Euclid’s lemma. Conversely, assume for contradiction that \( n \) is composite, i.e. \( n = uv \) for \( 1 < u, v < n \). Then by assumption, either \( n | u \) or \( n | v \). But since \( u, v < n \), this is absurd. \( \square \)

**Theorem 15 (Fund. theorem of arithmetic).** Each \( n \geq 2 \) is either a prime or can be uniquely (up to rearrangement of the factors) factorized as a product of primes.

**Proof.** Suppose that \( n \geq 2 \) has two prime factorizations: \( n = p_1 \cdots p_k \) and \( n = q_1 \cdots q_l \). Then \( p_i | q_i \) for some \( i \). In fact, up to rearranging the terms, we can suppose that \( p_1 | q_1 \). Since \( q_1 \) is prime, we conclude that \( p_1 = q_1 \) and our original equality reduces to \( p_2 \cdots p_k = q_1 \cdots q_l \). Repeating this argument a finite number of times, we can conclude that \( k = l \) and primes on both sides agree. \( \square \)

Observe that the argument above motivates the convention of excluding 1 from the list of prime numbers. We note the following application of the fundamental theorem of arithmetic, due to Euclid.

**Theorem 16.** Let \( p \) be prime, then \( \sqrt{p} \) is irrational.

**Proof.** Suppose for contradiction that \( \sqrt{p} = \frac{a}{b} \). Then \( pb^2 = a^2 \). Consider the prime decomposition \( b = p_1 \cdots p_k \). Then \( b^2 = p_1^2 \cdots p_k^2 \) has twice as many prime factors, and in particular, has an even number of prime factors. Hence if we look at the equation \( pb^2 = a^2 \), the left hand side has an odd number of prime factors, while the right hand side has an even number of prime factors, which is absurd. \( \square \)

**Exercise 21.** Generalize the proof above to show that if \( n \) is not a perfect square, then \( \sqrt{n} \) is irrational.
CHAPTER 2

Congruences

Fix $n \geq 1$. We can order the integers as follows

\[
\begin{array}{cccccccc}
-n & -n+1 & -n+2 & \ldots & -2 & -2 \\
0 & 1 & 2 & \ldots & n-2 & n-1 \\
2n & 2n+1 & 2n+2 & \ldots & 3n-2 & 3n-1 \\
\end{array}
\]

The (extended) Euclidean division algorithm tells us that each $a \in \mathbb{Z}$ can be written (in a unique way) as $a = qn + r$, where $q \in \mathbb{Z}$, and $r \in \{0, \ldots, n-1\}$. In particular, when divided by $n$, any number has its remainder (or residue) in the (finite) set $\{0, 1, \ldots, n-1\}$. We call two numbers $a, b$ that have the same residue congruent. Observe that then $a$ and $b$ differ by a multiple of $n$.

2.1. Gauss’ notation for congruences

Definition 22. Let $n \geq 1$. We say that $a$ is congruent to $b$ modulo $n$, written $a \equiv b \pmod{n}$, or even shorter, $a \equiv b \pmod{n}$, if $a$ and $b$ differ by a multiple of $n$. The positive integer $n$ is called the modulus.

In other words, $a \equiv b \pmod{n}$ if $n|\,(b-a)$. Notice that $n|\,(b-a)$ if and only if $n|(a-b)$: the equation $b-a = kn$ is equivalent to $a-b = (-k)n$.

Example 23. $63 \equiv 0 \pmod{3}$, $64 \equiv 1 \pmod{3}$, $7 \equiv -1 \pmod{8}$, $5^2 \equiv -1 \pmod{13}$.

Exercise 24. Show that if $a, b \in \mathbb{N}$ have the same parity (i.e. are either both odd, or both even), then $a \equiv b \pmod{2}$.

Theorem 17. Being congruent to modulus $n$ is an equivalence relation.

Proof. Recall that $\sim$ is an equivalence relation on a set $S$ if it is reflexive ($a \sim a$ for all $a \in S$), symmetric ($a \sim b$ if and only if $b \sim a$ for all $a, b \in S$), and transitive (if $a \sim b$ and $b \sim c$ then $a \sim c$). We only check that being congruent is transitive, and leave the rest to the reader. Suppose $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. By definition, there exist $k, l \in \mathbb{Z}$ such that $kn = (a-b)$ and $ln = (b-c)$. Hence $a-c = a-b + b-c = kn + ln = (k+l)n$. Thus $n|a-c$. □

As a result, congruences to same modulus behave (mostly) like equations.

Theorem 18. Fix $n \geq 1$. Suppose that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then

1. $a + c \equiv b + d \pmod{n}$ and $a - c \equiv b - d \pmod{n},$
2. $am \equiv bm \pmod{n}$ for all $m \in \mathbb{Z},$
3. $ac \equiv bd \pmod{n}.$
2. CONGRUENCES

Proof. By assumption $nk = a - b$ and $nl = c - d$, for some $k, l \in \mathbb{Z}$. Then $a + c - (b + d) = (a - b) + (c - d) = (k + l)n$, which proves the first assertion in (1). The second assertion is proven similarly. For (2), $n|b - a$ and hence $n|m(b - a)$ for all $m \in \mathbb{Z}$. For (3), we note that by by (2), $ac \equiv bc \pmod{n}$ and also $bc \equiv bd \pmod{n}$. Hence by transitivity, $ac \equiv bd \pmod{n}$. □

2.2. Applications

Gauss’ congruence notation is useful in devising obstructions on a number being of a certain form. For example,

**Proposition 25.** If $n \equiv 2 \pmod{4}$ or $n \equiv 3 \pmod{4}$ then $n$ is not a perfect square.

Proof. Let $n = a^2$. If $a = 2k$, then $n = 4k^2 \equiv 0 \pmod{4}$. Id $a = 2k + 1$, then $n = 4(k^2 + k) + 1 \equiv 1 \pmod{4}$. □

**Proposition 26.** If $n \geq 3$ is odd, then $n^2 + 1$ is not a prime.

Proof. $n$ is odd, hence $n \equiv 1 \pmod{2}$, hence $n^2 \equiv 1 \pmod{2}$ and $n^2 + 1 \equiv 0 \pmod{2}$. □

Another application: divisibility tests. For example,

**Proposition 27.** Let $n \in \mathbb{N}$. If the sum of the digits of $n$ is divisible by 3, then $n$ is divisible by 3.

Proof. Consider the decimal expansion of $n$; $n = a_0 + a_1 \cdot 10 + a_2 \cdot 100 + \ldots a_k \cdot 10^k$, or,

$$n = a_0 + a_1 \cdot (3^2 + 1) + a_2(3^1 + 1) + \ldots a_k \cdot (3^{2k} + 1) \equiv a_0 + a_1 + a_2 + \cdots + a_k \pmod{3}.$$

If the sum of the digits $a_0 + a_1 + \ldots a_k \equiv 0 \pmod{3}$, then $n \equiv 0 \pmod{3}$. □

Remark 28. The same argument works with 9 instead of 3.

**Proposition 29.** If the last two digits of $n$ are divisible by 4, then $n$ is divisible by 4.

Proof. Consider the decimal expansion of $n$;

$$n = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \ldots a_k \cdot 10^k = a_0 + a_1 \cdot (2 \cdot 5) + a_2 \cdot (2^2 \cdot 5^2) + \ldots a_k \cdot (2^k \cdot 5^k) = a_0 + a_1 \cdot 10 + a_2 \cdot (4 \cdot 5^2) + \ldots a_k \cdot (4 \cdot 2^{k-2} \cdot 5^k) \equiv a_0 + a_1 \cdot 10 \pmod{4}.$$

□

**Exercise 30.** Show that if the alternating sum of the digits of $n$ is a multiple of 11, then $n$ is a multiple of 11.
2.3. Arithmetic properties

One can generalize Theorem 18 to show that given \( a_i \equiv b_i \, (n) \), \( i = 1, \ldots, k \), then
\[
a_1 + \cdots + a_k \equiv c_1 + \cdots + c_k \, (n), \quad a_1 \cdots a_k \equiv c_1 \cdots c_k \, (n).
\]

However the cancellation law \((ab \equiv ac \implies b \equiv c)\) does not always hold in congruence equations.

Example 31. \( 12 \equiv 24 \, (10) \) and \( 2 \cdot 6 = 12, \, 7 \cdot 6 = 42, \) but \( 2 \not\equiv 7 \, (10) \).

Proposition 32. If \( ab \equiv ac \, (n) \) and \( (a, n) = 1 \) then \( b \equiv c \, (n) \).

Proof. We will see that this is really only a reformulation of Euclid’s lemma. Indeed, \( ab \equiv ac \, (n) \iff n|a(b - c) \) and since \( (a, n) = 1, \, n|(b - c) \) and this is equivalent to \( b \equiv c \, (n) \). \( \square \)

And in general,

Proposition 33. If \( ab \equiv ac \, (n) \) then \( b \equiv c \, \left( \frac{n}{(a,n)} \right) \).

Proof. Let \( d := (a, n) \) and \( n = kd, \, a = ld \). Then \( (l, k) = 1 \). (Why is this true?) With these new variables, \( ab \equiv ac \, (n) \) becomes \( ldb \equiv ldc \, (kd) \). Observe that this is equivalent to \( lb \equiv lc \, (k) \). Since \( (k, l) = 1 \), the statement follows from Proposition 32. \( \square \)

We will denote by \( \mathbb{Z}_n \) the set of distinct congruences \( x \equiv 0, 1, \ldots, n - 1 \, (n) \). (This notation, as the discussion about to follows, will be familiar to anyone who took abstract algebra.) We now have seen that \( \mathbb{Z}_n \) is closed under addition and multiplication. It is easy to see that \( a + x \equiv 0 \, (n) \) has a solution — take \( x \equiv -a \, (n) \) — and that all solutions are congruent to it mod \( n \). What about \( ax \equiv 1 \, (n) \)? If \( x \) is a solution, then it is necessarily congruent to one of \( 1, 2, \ldots, n - 1 \). So we only have finitely many options to check.

Example 34. Consider the following two examples.

1. \( 3x \equiv 1 \, (5) \). Then \( 3 \cdot 2 = 6 \equiv 1 \, (5) \) is a solution.
2. \( 3x \equiv 1 \, (6) \). Here there are no solutions. Indeed, \( 3 \not\equiv 1 \, (6), \, 3 \cdot 2 \equiv 0 \, (6), \, 3 \cdot 3 \equiv 3 \, (6), \, 3 \cdot 4 = 12 \equiv 0 \, (6), \, 3 \cdot 5 \equiv 3 \, (6) \).

Proposition 35. \( ax \equiv 1 \, (n) \) has a solution if and only if \( (a, n) = 1 \).

Proof. Suppose that \( x \) is a solution to \( ax \equiv 1 \, (n) \), and suppose for contradiction that \( d := (a, n) > 1 \). Then since \( d|n \) and \( n|(ax - 1) \), \( ax \equiv 1 \, (d) \). Since \( d|a \) also holds, \( ax \equiv 0 \, (d) \), and we are left with \( 0 \equiv 1 \, (d) \), which is absurd.

Conversely, suppose that \( (a, n) = 1 \). By Corollary 15 (Bézout’ Lemma), there exist \( u, v \in \mathbb{Z} \) such that \( au + nv = 1 \). Then \( au \equiv 1 \, (n) \) and \( u \) is a solution to \( ax \equiv 1 \, (n) \). \( \square \)

Exercise 36. Show that more generally, \( ax \equiv b \, (n) \) has a solution if and only if \( (a, n)|b \).
The only \( a \in \mathbb{Z} \) having a multiplicative inverse, i.e. for which \( ax = 1 \) has a solution, are \( a = \pm 1 \). And in particular, these are self-reciprocal (their own inverses). Proposition 35 above tells us that in \( \mathbb{Z}_n \) there are
\[
\varphi(n) = \# \{1 \leq a < n : (a, n) = 1\}
\]
elements that admit a multiplicative inverse. (The function \( \varphi(n) \) is called Euler’s totient function, and we will meet it again...)

Example 37. Check that \( \varphi(4) = 2 \), \( \varphi(17) = 16 \), and that in general \( \varphi(p) = p - 1 \).

Question: How many elements in \( \mathbb{Z}_n \) are self-reciprocal? For the moment, we will answer this for \( n = p \) prime. That is, how many \( a \in \mathbb{Z}_p \) satisfy
\[
a^2 \equiv 1 \ (p) \iff a^2 - 1 = (a - 1)(a + 1) \equiv 0 \ (p) \implies a \equiv 1 \ (p) \text{ and } a \equiv -1 \ (p),
\]
hence there are only two self-reciprocal elements mod \( p \): 1 and \( p - 1 \). Using this, we can present Gauss’ proof of Wilson’s theorem:

**Theorem 19 (Wilson’s theorem).** \( p \) is a prime if and only if \( (p - 1)! \equiv -1 \ (p) \).

**Proof.** If \( p = 2 \), this is clear. Suppose that \( p > 2 \). Suppose that \( p \) is prime. By the discussion above, each of \( 1, 2, \ldots, p - 1 \) has a (unique) multiplicative inverse among \( 1, \ldots, p - 1 \). Moreover, in this set, only 1 and \( p - 1 \) are self-reciprocal. Consider the product \( 2 \cdot 3 \cdot \cdots (p - 2) \). This is a product of \( p - 2 - 1 = p - 3 \), i.e., an even number of factors. If we pair each factor with its reciprocal, we obtain that
\[
(p - 2)! = 2 \cdot 3 \cdot \cdots (p - 2) \equiv 1 \ (p).
\]
And so multiplying both sides by \( p - 1 \): \( (p - 1)! \equiv p - 1 \equiv -1 \ (p) \).

Conversely, assume for contradiction that \( p \) has a non-trivial divisor, \( d \mid p \). Then \( (p - 1)! \equiv -1 \ (d) \), but since \( d < p \), \( (p - 1)! \equiv 0 \ (d) \). We are left with \( 0 \equiv -1 \ (d) \) which is absurd for \( d \geq 2 \). \( \square \)

We have a new primality test! ...but considering it requires computing a factorial, this is rather only of theoretical value. In the next section, we see another similar primality test – via Fermat’s little theorem – that as practical significance.

**2.4. Fermat and Euler theorems**

**Theorem 20 (Fermat’s little theorem (1640)).** Let \( p \) be a prime, and \( (a, p) = 1 \). Then
\[
a^{p-1} \equiv 1 \ (p).
\]

**Proof.** We present a proof of Ivory (1806): \( a, 2a, 3a, \ldots, (p-1)a \) are congruent (in some order) to \( 1, 2, \ldots, p-1 \). In fact this is a one-to-one correspondence: if \( ja \equiv ka \ (p) \) then since \( (a, p) = 1, j \equiv k \ (p) \), but \( 1 \leq j, k \leq p - 1 \), hence \( j = k \).) Then
\[
a(2a)(3a) \cdots ((p-1)a) \equiv (p-1)! \ (p)
\]
and
\[
a(2a)(3a) \cdots ((p-1)a) = (p-1)!a^{p-1}.
\]
Thus \((p - 1)!a^{p-1} \equiv (p - 1)! \pmod{p}\) and since \((p, (p - 1)!)\), we may divide \((p - 1)!\) from both sides. 

\[\text{Remark 38. For applications (as we will see an example below), it is sometimes useful to keep in mind that } a^{p-1} \equiv 1 \pmod{p} \iff a^p \equiv a \pmod{p}.\]

**Primality testing.** We can rule out that a large number is prime using Fermat’s Little Theorem (how?). Conversely, a number \(n\) for which \((a, n) = 1\) and \(a^{n-1} \equiv 1 \pmod{n}\) has a good chance to be prime, but this is not sufficient. An example is \(561 = 3 \cdot 11 \cdot 17\). We test with Fermat using repeated squaring to reduce the power to compute. First note \(560 = 2 \cdot 280 = 2 \cdot 2 \cdot 140 = 2^3 \cdot 70 = 2^4 \cdot 35\). Good enough, \(2^{35}\) is computable. In fact, 

\[2^{35} \equiv 263 \pmod{561}.
\]

Squaring both sides, 

\[2^{70} \equiv 166 \pmod{561},\]

and repeating the process enough many times: \(2^{140} \equiv 67 \pmod{561}, 2^{280} \equiv 1 \pmod{561}\), and from here it follows that 

\[2^{560} \equiv 1 \pmod{561}.
\]

Hence 561 is a ‘false positive’. We call such numbers **pseudo-primes** (or Carmichael numbers) – 561 is the smallest pseudo-prime.

**Solving linear congruence equations.** Earlier, we have seen that the equation 
\[ax \equiv b \pmod{p},\]
for \(p\) prime, has a solution. Fermat’s Little Theorem gives us a simple way of finding this solution: multiply both sides of the congruence equation by \(a^{p-2}\), then using that \(a^{p-1} \equiv 1\),

\[ax \equiv b \pmod{p} \implies x \equiv a^{p-2}b \pmod{p}.
\]

**Example 39.** Let’s solve \(5x \equiv 2 \pmod{17}\). Applying Fermat, \(x \equiv 5^{15} \cdot 2 \pmod{17}\) is a solution. We now want to find the remainder of \(5^{15}\) when divided by 17:

\[5^{15} = 25^7 \cdot 5 \equiv 8^7 \cdot 5 = 64^3 \cdot 5 \equiv (-4)^3 \cdot 5 = -16 \cdot 5 \equiv 1 \cdot 7 = 7 \pmod{17}.
\]

hence \(x \equiv 5^{15} \cdot 2 \equiv 14 \pmod{17}\).

From this, can we infer the case of general modulus \(n\) ? This is Euler’s generalization of Fermat’s theorem:

**Theorem 21 (Euler’s theorem, 1760).** If \((x, n) = 1\), then

\[x^{\varphi(n)} \equiv 1 \pmod{n},
\]
where \(\varphi(n) = \#\{0 \leq m < n : (m, n) = 1\}\) is Euler’s totient function.

**Remark 40.** We have already met Euler’s totient function once. For now, let’s simply observe that if \(p\) is prime, \(\varphi(p) = p - 1\). So this indeed generalizes Fermat’s theorem.

**Proof.** We apply the same argument we applied to prove Fermat’s Little Theorem. [COMPLETE]