M328K – INTRODUCTION TO NUMBER THEORY – FALL 2005

GERGELY HARCOS

Principle of Induction. Some equivalent and frequently used formulations:

(1) If a given statement holds for the number 1 and the validity of the statement is inherited from any positive integer to its successor then the statement holds for all positive integers.
(2) If the validity of a given statement for any given positive integer follows from the validity of the statement for all smaller positive integers then the statement holds for all positive integers.
(3) If any positive integer of a given property gives rise to a smaller positive integer with the same property, then there is no positive integer of that property.
(4) If a given property is satisfied by some positive integer then there is a smallest positive integer with that property.

Remark 1. Formulation (1) is the method of mathematical induction, due to Augustus de Morgan (1806–1871). Formulation (2) is the method of complete induction, due to Richard Dedekind (1831–1916). Formulation (3) is the method of infinite descent, due to Pierre de Fermat (1601–1665). Formulation (4) essentially says that the standard ordering on the positive integers is a well-ordering, a notion introduced by Georg Cantor (1845–1918).

1. Divisors and multiples

Definition 1. $a \mid b$ if there is a' such that $b = aa'$. We say that a is a *divisor* of b, and b is a *multiple* of a.

Remark 2. Divisors come in pairs.

Example 1. $a \mid 0$. $\pm a \mid a$. $\pm 1 \mid a$. If $a \mid 1$ then $a = \pm 1$.

Proposition 1. *For arbitrary a, b, c, x, y we have the following.*

(1) *If $a \mid b$ and $b \mid c$ then $a \mid c$.*
(2) *If $a \mid b$ then $ac \mid bc$.*
(3) *If $ac \mid bc$ then $a \mid b$ or $c = 0$.*
(4) *If $a \mid b$ then $a \mid bc$.*
(5) *If $a \mid b$ and $a \mid c$ then $a \mid b \pm c$.*
(6) *If $a \mid b$ and $a \mid c$ then $a \mid bx + cy$.*

Theorem 1. *For arbitrary a and positive b there is a unique decomposition*

$$a = bq + r, \qquad 0 \le r < b.$$

Proof. First we show that the claimed decomposition exists. As b is positive, there are nonnegative numbers of the form $a - bq$. Let $r = a - bq$ be the least such nonnegative number (so we have specified q and r). The number $r - b$ is less than

r (since b is positive) and can be written as $a - b(q+1)$. Hence $r - b$ must be negative, so in fact $0 \leq r < b$ as needed.

Second we show that the claimed decomposition is unique. This means that

$$bq + r = bq' + r', \qquad 0 \leq r, r' < b$$

can only hold when $q = q'$ and $r = r'$. Indeed, $b(q-q') = r' - r$ lies strictly between $-b$ and b, hence $-1 < q - q' < 1$ (since b is positive), hence $q = q'$, hence $r = r'$. □

Remark 3. We say that when a is divided by b, q is the *quotient* and r is the *residue*. From the proof it is easy to extract an algorithm that determines r.

Algorithm 1. Input: $a \geq 0$ and $b > 0$.

```
(1) If $a < b$ then output $a$.
(2) Replace $a$ by $a - b$.
(3) Go to (1).
```

Proposition 2. *For any input $a \geq 0$ and $b > 0$, Algorithm 1 returns an r such that $0 \leq r < b$ and $b \mid a - r$.*

Proof. We fix $b > 0$ and proceed by complete induction on a. That is, we assume that the statement is true for all $a' < a$ in place of a. If $a < b$ then the algorithm returns a in step (1). This output has the required properties, since $0 \leq a < b$ by assumption and $a - a = 0$ is a multiple of b. If $a \geq b$ then step (1) is skipped and then steps (2) and (3) are performed. After that the algorithm does exactly what it would do for the input $a' := a - b \geq 0$ and $b > 0$. As $a' < a$, the induction hypothesis tells us that the algorithm returns an r such that $0 \leq r < b$ and $b \mid a' - r$. But $a - r = (a' - r) + b$, hence $b \mid a - r$ by part (5) of Proposition 1. □

Definition 2. If a or b is nonzero then (a, b) is the *greatest common divisor* of a and b. If a and b are zero then (a, b) is zero. If $(a, b) = 1$ then we say that a and b are *coprime* or *relatively prime*.

Definition 3. If a and b are nonzero then $[a, b]$ is the positive *least common multiple* of a and b. If a or b is zero then $[a, b]$ is zero.

Example 2. $(a, 0) = |a|$. $(\pm a, \pm b) = (a, b)$. $[a, 0] = 0$. $[\pm a, \pm b] = [a, b]$.

Proposition 3. *For arbitrary a, b, q we have*

$$(a - bq, b) = (a, b).$$

Proof. We shall assume that a and b are not both zero for otherwise the statement is trivial. If $d \mid a$ and $d \mid b$ then $d \mid a - bq$ by part (6) of Proposition 1. If $d \mid a - bq$ and $d \mid b$ then $d \mid a$ also by part (6) of Proposition 1. This shows that a and b have the same common divisors as $a - bq$ and b. In particular, their greatest common divisor is the same. □

Algorithm 2. Input: $a, b \geq 0$ such that $a + b > 0$.

```
(1) If $a < b$ then flip the values of $a, b$.
(2) If $b = 0$ then output $a$.
(3) Replace $a$ by $a - b$.
(4) Go to (1).
```

Theorem 2 (Euclid)**.** *For any input $a, b \geq 0$ such that $a + b > 0$, Algorithm 2 returns (a, b). Moreover, there exist x, y such that $(a, b) = ax + by$.*

Proof. We proceed by complete induction on $a+b$. That is, we assume the validity of the statement for any input $a', b' \geq 0$ satisfying $0 < a'+b' < a+b$. If $a < b$ then step (1) is performed and after that the algorithm does exactly what it would do for the input $a' := b$ and $b' := a$ which satisfies $a' \geq b' \geq 0$ and $a'+b' = a+b$. Moreover, $(a', b') = a'x' + b'y'$ is the same as $(a, b) = ay' + bx'$. Therefore we can certainly assume that $a \geq b$. In this case step (1) is skipped. If $b = 0$ then the algorithm returns a in step (2) which of course equals (a, b). Moreover, $(a, b) = 1.a + 0.b$. Therefore we can further assume that $a \geq b > 0$. Then step (2) is also skipped and steps (3) and (4) are performed. After that the algorithm does exactly what it would do for the input $a' := a - b \geq 0$ and $b' := b > 0$. As $0 < a' + b' = a < a + b$, the induction hypothesis tells us that the algorithm returns (a', b') and also that $(a', b') = a'x' + b'y'$ for some x', y'. But $(a', b') = (a-b, b) = (a, b)$ by Proposition 3, hence the algorithm indeed returns (a, b) and also

$$(a, b) = (a', b') = a'x' + b'y' = (a-b)x' + by' = ax' + b(y' - x') = ax + by$$

upon setting $x := x'$ and $y := y' - x'$. □

Remark 4. Algorithms 1 and 2 are called the Division Algorithm and the Euclidean Algorithm. It is clear that these algorithms are closely related. In fact, it is straightforward to check that step (3) in the Euclidean Algorithm could be replaced by the more efficient step

(3') Replace a by the output r of Algorithm 1 for the input $a \geq 0$ and $b > 0$.

Remark 5. The Euclidean Algorithm and the proof of Theorem 2 highlight the following property. Any pair $\langle a, b\rangle$ with $a, b \geq 0$ and $a + b > 0$ can be moved to $\langle (a, b), 0\rangle$ by only using moves of the type $\langle a, b\rangle \to \langle b, a\rangle$ (when $a < b$) and $\langle a, b\rangle \to \langle a - b, b\rangle$ (when $a \geq b > 0$). This observation allows a kind of "Euclidean Induction" for proving certain statements $P(a, b)$ involving such pairs. Namely, for the universal validity of $P(a, b)$ it suffices to show that

(1) $P(a, b)$ holds true when $b = 0$;
(2) $P(a, b)$ follows from $P(b, a)$ when $a < b$;
(3) $P(a, b)$ follows from $P(a - b, b)$ when $a \geq b > 0$.

Remark 6. In the language of linear algebra the above two moves are linear maps of determinants -1 and $+1$, respectively. Any successive application of these moves is realized by right multiplication by a matrix $\begin{pmatrix} x & w \\ y & z \end{pmatrix}$ of determinant ± 1 according to whether an even or an odd number of flips were applied. If this matrix arises from the steps performed by the Euclidean Algorithm on a particular pair $\langle a, b\rangle$, then the entries x, y can be identified with those in Theorem 2, while the entries w, z are equal to $\mp b/(a, b), \pm a/(a, b)$ according to the parity of the number of flips performed.

Theorem 3. *For arbitrary a, b, n the equation*

$$ax + by = n$$

has a solution x, y if and only if (a, b) divides n.

First proof (using Theorem 2). We shall assume that a and b are not both zero for otherwise the statement is trivial. The "only if" part follows from part (6) of Proposition 1. To prove the "if" part it suffices to show that there are x, y such that $(a,b) = ax + by$. By Example 2 we may restrict ourselves to the case when $a, b \geq 0$. Then the statement is part of Theorem 2. □

Second proof (using Theorem 1). We shall assume that a and b are not both zero for otherwise the statement is trivial. Then at least one of $\pm a, \pm b$ is positive, so there certainly are positive numbers of the form $ax + by$. Let $d = ax_0 + by_0$ be the least such positive number. It is clear that each multiple of d can be written as $ax + by$. We claim that the converse is also true, that is, any number $n = ax_1 + by_1$ is a multiple of d. By Theorem 1 there is a unique decomposition $n = dq + r$ where $0 \leq r < d$. Observe that r is of the form $ax + by$:

$$r = n - dq = a(x_1 - x_0 q) + b(y_1 - y_0 q).$$

This shows that r cannot be positive (since it is less than d), hence $r = 0$ and $d \mid n$ as claimed. In particular, taking $n = a$ and $n = b$ shows that d is a common divisor of a and b. We claim that d is the greatest common divisor, that is, $d = (a,b)$. To see this let c be any common divisor of a and b. Then, from the representation $d = ax_0 + by_0$ and part (6) of Proposition 1 it follows that c is a divisor of d, so it cannot be greater than d. □

Corollary 1. *For arbitrary a, b, c we have*

$$(ca, cb) = |c|(a,b).$$

Proof. We shall assume that c is nonzero and also that a or b is nonzero for otherwise the statement is trivial. By Theorem 3 the set of numbers of the form $cax + cby$ agrees with the set of multiples of (ca, cb). Since $cax + cby = c(ax + by)$, the same corollary shows that this set also agrees with the set of multiples of $c(a,b)$. Therefore (ca, cb) and $|c|(a,b)$ are multiples of each other. These numbers are positive, hence they are equal. □

Remark 7. The analogous relation

$$[ca, cb] = |c|[a,b]$$

holds for much simpler reasons.

Theorem 4 (Euclid)**.** *Let a and b be arbitrary.*

(1) *Any common multiple of a and b is a multiple of $[a,b]$.*
(2) *Any common divisor of a and b is a divisor of (a,b).*
(3) $(a,b)[a,b] = |ab|$.

First proof (using Theorem 1). If $a = 0$ then $(a,b) = |b|$, $[a,b] = 0$, whence all statements are trivial. Similarly, the case of $b = 0$ is trivial. Therefore we shall assume that a and b are nonzero. Switching the sign of a or b does not alter the statements, therefore it suffices to prove the theorem for positive a, b.

(1): Put $m := [a,b]$. Assume that c is a common multiple of a and b. Let $c = mq + r$ with $0 \leq r < m$ according to Theorem 1. By (6) of Proposition 1 $a \mid c$ and $a \mid m$ implies that $a \mid c - mq$, that is, $a \mid r$. Similarly, $b \mid r$. Therefore r is a common multiple of a and b, less than m. This shows that r cannot be positive, so $r = 0$, so $m \mid c$.

(2)&(3): Applying (1) for $c = ab$ it follows that $m \mid ab$. In other words, $ab = dm$ for some positive d. Since $a = d(m/b)$, d is a divisor of a. Similarly, d is a divisor of b. That is, d is a common divisor of a and b. Now let c be an arbitrary common divisor of a and b. Then $ab/c = a(b/c) = b(a/c)$ is a common multiple of a and b.

By (1) it follows that $ab/c = mk$ for some positive k. Now $d = ab/m = ck$ shows that c is a divisor of d. We have showed that any common divisor of a and b is a divisor of d which itself is a common divisor. In particular, $d = (a, b)$. □

Second proof (using Theorem 2). As observed in the first proof, we can assume that a, b are positive.

(2): Put $d := (a, b)$. Assume that c is a common divisor of a and b. By Theorem 2 there is a representation $d = ax + by$ with some x, y. This in combination with part (6) of Proposition 1 shows that c is a divisor of d.

(1)&(3): By part (4) of Proposition 1 $d \mid ab$. In other words, $ab = dm$ for some positive m. Since $m = a(b/d)$, m is a multiple of a. Similarly, m is a multiple of b. That is, m is a common multiple of a and b. Now let c be an arbitrary common multiple of a and b. By part (2) of Proposition 1 we have $ab \mid ac$ and also $ab \mid bc$. By part (6) of Proposition 1 it follows that $ab \mid acx + bcy$. That is, $ab \mid dc$. But $ab = dm$, so that in fact $dm \mid dc$. By (3) of Proposition 1 $m \mid c$ (since d is positive). We have showed that any common multiple of a and b is a multiple of m which itself is a common multiple. In particular, $m = [a, b]$. □

Theorem 5 (Euclid). *If a, b are not both zero then $ax = by$ if and only if $x = kb/(a, b)$, $y = ka/(a, b)$ for some k.*

Proof. If $a = 0$ then $b \neq 0$, $b/(a, b) = \pm 1$, hence the statement reduces to the obvious claim that $0 = by$ if and only $y = 0$. Therefore we shall assume that $a \neq 0$. For similar reasons we shall assume that $b \neq 0$. If $x = kb/(a, b)$, $y = ka/(a, b)$ for some k then certainly $ax = by$. Now let x, y arbitrary such that $ax = by$. Then $ax = by$ is a common multiple of a, b, hence it equals $k[a, b]$ for some k by part (1) of Theorem 4. Combining with part (3) of Theorem 4, this means that $ax = by = kab/(a, b)$, that is, $x = kb/(a, b)$, $y = ka/(a, b)$. □

Remark 8. Theorem 4 and its first proof as well as Theorem 5 can be described in geometric terms. Let us assume that a and b are positive. Common multiples of a and b can be written as $ax = by$ and hence correspond bijectively to the lattice vectors $\langle x, y\rangle$ of slope a/b. Of these vectors there is a shortest with positive coordinates, call it $\langle x_0, y_0\rangle$. Statement (1) says that any lattice vector of slope a/b is a multiple of $\langle x_0, y_0\rangle$. Common divisors c of a and b correspond bijectively to the lattice vectors $\langle b/c, a/c\rangle$ dividing $\langle b, a\rangle$. Statement (2) says that $\langle x_0, y_0\rangle$ is a divisor of $\langle b, a\rangle$ which divides all the divisors of $\langle b, a\rangle$. Statement (3) says that $\langle x_0, y_0\rangle = \langle b/(a, b), a/(a, b)\rangle$. Theorem 5 summarizes that the nonzero multiples of $\langle b/(a, b), a/(a, b)\rangle$ are exactly the lattice vectors of slope a/b. It also expresses the fact that the fraction a/b has a unique representation in lowest terms with a positive denominator, namely y_0/x_0, where $x_0 = b/(a, b)$ and $y_0 = a/(a, b)$.

Corollary 2. *If a, b are not both zero and (a, b) divides n then the solutions of*

$$ax + by = n$$

are of the form $x = x_0 + kb/(a, b)$ and $y = y_0 - ka/(a, b)$ with fixed x_0, y_0.

Proof. By Theorem 3 there exists a solution x_0, y_0 of the equation. Let us fix this solution. Then the equation can be written as $ax + by = ax_0 + by_0$, that is, $a(x - x_0) = b(y_0 - y)$. By Theorem 5 this holds true if and only if $x - x_0 = kb/(a, b)$ and $y_0 - y = ka/(a, b)$. □

Theorem 6. *If $(a,b)=1$ and $a \mid bc$ then $a \mid c$.*

First proof (using Theorem 5). As $bc=ad$ for some d it follows from Theorem 5 that $c=ak$ and $d=bk$ for some k. In particular, $a \mid c$. □

Second proof (using Theorem 2). Clearly, a is a common divisor of ac and bc. By part (6) of Proposition 1 $a \mid acx+bcy$ for any x,y. By Theorem 2 we can choose x,y so that $ax+by=1$, and then $a \mid c$ follows. □

Theorem 7 (Euclid)**.** *If $(a,n)=1$ and $(b,n)=1$ then $(ab,n)=1$.*

First proof (using Theorem 6). If $n=0$ then $a,b=\pm 1$, so the statement is obvious. We can therefore assume that n is nonzero. Put $d:=(ab,n)$. As $d \mid n$, every common divisor of a and d is also a common divisor of a and n. This shows that $(a,d)=1$. In addition, $d \mid ab$, so by Theorem 6 we can conclude that $d \mid b$. Therefore d is a positive common divisor of b and n, hence $d=1$. □

Second proof (using Theorem 2). By Theorem 2 there are integers x_1,y_1,x_2,y_2 such that

$$ax_1+ny_1=1 \quad \text{and} \quad bx_2+ny_2=1.$$

Multiplying these equations we get

$$abx_1x_2+nby_1x_2+nax_1y_2+n^2y_1y_2=1.$$

In particular,

$$x:=x_1x_2 \quad \text{and} \quad y:=by_1x_2+ax_1y_2+ny_1y_2$$

solve the equation

$$abx+ny=1.$$

By part (6) of Proposition 1 (ab,n) divides the left hand side, hence $(ab,n)=1$. □

2. Unique factorization

Definition 4. An integer $n>1$ is called *composite* if it can be decomposed as $n=ab$ with $a,b>1$. An integer $n>1$ that is not composite is called *prime*.

Remark 9. In other words, $n>1$ is prime if and only if 1 and n are its only positive divisors.

Proposition 4. *Every integer $n>1$ is a product of primes.*

Proof. We proceed by complete induction on n. If n is prime then the statement is valid. Otherwise n decomposes as $n=ab$ with $a,b>1$. Observe that $a,b<n$, therefore a,b are products of primes by the induction hypothesis. Hence n is a product of primes. □

Corollary 3. *Every integer $n>1$ has a prime divisor.* □

Theorem 8 (Euclid)**.** *There are infinitely many prime numbers.*

Proof. Let $p_1,p_2,\dots,p_n$ be any finite sequence of positive integers. By Corollary 3 there is a prime p dividing $p_1p_2\dots p_n+1$. Clearly, p does not divide $p_1p_2\dots p_n$, therefore p is not among $p_1,p_2,\dots,p_n$. This shows that no finite sequence can contain all prime numbers. □

Proposition 5. *If p is prime and a is arbitrary then either $p \mid a$ or $(a,p)=1$.*

Proof. As (a, p) is a positive divisor of p, either $(a, p) = 1$ or $(a, p) = p$. The second case is equivalent to $p \mid a$. □

Theorem 9 (Euclid)**.** *If p is prime and $p \mid ab$ then $p \mid a$ or $p \mid b$.*

Proof. Assume that $p \nmid a$. Then $(a, p) = 1$ by Proposition 5, hence $p \mid b$ by Theorem 6. □

Theorem 10. *Every integer $n > 1$ can be written uniquely as a product of primes, apart from the order of the factors.*

First proof (using Theorem 9). By Proposition 4 it suffices to show that there are no two different decompositions of n as a product of primes, apart from the order of the factors. Let

$$n = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$$

be two such decompositions. By reordering/renaming the factors we can achieve that $p_1 \le p_2 \le \dots \le p_r$ and $q_1 \le q_2 \le \dots \le q_s$. We need to show that $r = s$ and $p_i = q_i$ for each $i = 1, 2, \dots, r = s$. We prove this reduced statement by complete induction on n. Let p be the smallest prime divisor of n. By Theorem 9 p divides one of the p_i's, hence it equals one of the p_i's. But then p equals the smallest of the p_i's, that is, $p = p_1$. The same reasoning shows that $p = q_1$. Therefore $p_1 = q_1 = p$. If $n = p$ then $r = s = 1$ and we are done. Otherwise $n/p > 1$, hence $r, s > 1$ and

$$n/p = p_2 p_3 \dots p_r = q_2 q_3 \dots q_s.$$

By the induction hypothesis $r - 1 = s - 1$ and $p_i = q_i$ for $i = 2, 3, \dots, r = s$. □

Second proof (using only induction). The heart of the previous proof was the deduction, with the help of Theorem 9, that $p = p_1$. We shall redo this step without using Theorem 9. Let us assume that $p \neq p_1$. Then certainly $r > 1$ and $p < p_1$ as p is the smallest prime divisor of n. Consider the product $n' := (p_1 - p)p_2 p_3 \dots p_r$. Observe that $1 < n' < n$ and $p \mid n'$. By Proposition 4 there are primes $p'_1, p'_2, \dots, p'_t$ and $p''_1, p''_2, \dots, p''_u$ such that

$$n'/p = p'_1 p'_2 \dots p'_t \qquad \text{and} \qquad p_1 - p = p''_1 p''_2 \dots p''_u.$$

Then

$$n' = p p'_1 p'_2 \dots p'_t = p''_1 p''_2 \dots p''_u p_2 p_3 \dots p_r$$

are two decompositions of n' as a product of primes. By the induction hypothesis these two decompositions only differ in the order of the factors. In particular, p equals one of the factors on the right hand side. As $p < p_i$ for all i, we must have $p = p''_j$ for some j. This implies $p \mid p_1 - p$, hence $p \mid p_1$, a contradiction to $1 < p < p_1$. □

Corollary 4. *Every integer $n > 1$ can be written uniquely as $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, where $p_1 < p_2 < \dots < p_r$ are distinct primes and the exponents α_i are positive.* □

Theorem 11. *Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, where $p_1 < p_2 < \dots < p_r$ are distinct primes and the exponents α_i are positive. If $d = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}$ with $0 \le \beta_i \le \alpha_i$ then d is a positive divisor of n. Moreover, every positive divisor d of n can be written uniquely in this form.*

Proof. If $d = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}$ with $0 \leq \beta_i \leq \alpha_i$, then the integers $\beta_i' := \alpha_i - \beta_i$ are nonnegative, hence $d' := p_1^{\beta_1'} p_2^{\beta_2'} \dots p_r^{\beta_r'}$ is an integer satisfying $n = dd'$. This shows that d is a positive divisor of n.

Now let d be an arbitrary positive divisor of n. By definition $n = dd'$ for some positive d'. Let $q_1 < q_2 < \dots < q_s$ be the primes dividing d or d'. By Proposition 4

$$d = q_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s} \qquad \text{and} \qquad d' = q_1^{\beta_1'} q_2^{\beta_2'} \dots q_s^{\beta_s'}$$

for some nonnegative exponents β_i and β_i'. Observe that $\beta_i + \beta_i'$ is positive for each i (since q_i divides d or d'), and also

$$n = dd' = q_1^{\beta_1+\beta_1'} q_2^{\beta_2+\beta_2'} \dots q_s^{\beta_s+\beta_s'}.$$

By Theorem 10 it follows that $r = s$, and $q_i = p_i$, $\beta_i + \beta_i' = \alpha_i$ for all i. In particular, $0 \leq \beta_i \leq \alpha_i$, whence d has the form claimed. It also follows from Theorem 10 that the exponents β_i are uniquely determined by d. □

Definition 5. The number of positive divisors of n is denoted by $\tau(n)$. The sum of positive divisors is denoted by $\sigma(n)$.

Corollary 5. *Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, where $p_1 < p_2 < \dots < p_r$ are distinct primes and the exponents α_i are positive. Then*

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_r + 1).$$

□

Theorem 12. *Let*

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} \qquad \textit{and} \qquad b = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r},$$

where $p_1 < p_2 < \dots < p_r$ are distinct primes and the exponents α_i, β_i are nonnegative. Then

$$(a, b) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \dots p_r^{\min(\alpha_r,\beta_r)}$$
$$[a, b] = p_1^{\max(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)} \dots p_r^{\max(\alpha_r,\beta_r)}.$$

Proof. By Theorem 11 the common divisors of a, b are exactly the divisors of

$$p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \dots p_r^{\min(\alpha_r,\beta_r)},$$

while the common multiples of a, b are exactly the multiples of

$$p_1^{\max(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)} \dots p_r^{\max(\alpha_r,\beta_r)}.$$

Therefore these expressions agree with (a, b) and $[a, b]$, respectively. □

Remark 10. Note that Theorem 12 and its proof imply Theorem 4.

Corollary 6. *Let k be positive. Then for arbitrary a, b we have*

$$(a^k, b^k) = (a, b)^k \qquad \textit{and} \qquad [a^k, b^k] = [a, b]^k.$$

Proof. We can assume that a and b are nonzero for otherwise the statement is obvious. Switching the sign of a or b does not alter the statement, therefore we can further assume that a and b are positive. Then the statement follows at once from Theorem 12 upon noting that

$$\min(k\alpha, k\beta) = k \min(\alpha, \beta) \qquad \text{and} \qquad \max(k\alpha, k\beta) = k \max(\alpha, \beta).$$

□

Theorem 13. *Let m and n be relatively prime. If d is a positive divisor of m and e is a positive divisor of n then de is a positive divisor of mn. Moreover, every positive divisor of mn can be written uniquely in this form.*

Proof. Let

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} \qquad \text{and} \qquad n = q_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s}$$

be the unique prime factorization of m and n. As m and n are relatively prime, neither of the primes p_i equal any of the primes q_j, therefore the unique prime factorization of mn reads

$$mn = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} q_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s}$$

with distinct primes p_i and q_j. By Theorem 11 the numbers

$$p_1^{\gamma_1} p_2^{\gamma_2} \dots p_r^{\gamma_r} q_1^{\delta_1} q_2^{\delta_2} \dots q_s^{\delta_s}$$

with $0 \le \gamma_i \le \alpha_i$ and $0 \le \delta_j \le \beta_j$ are positive divisors of mn, and every positive divisor of mn can be written uniquely in this form. By introducing the notation

$$d := p_1^{\gamma_1} p_2^{\gamma_2} \dots p_r^{\gamma_r} \qquad \text{and} \qquad e := q_1^{\delta_1} q_2^{\delta_2} \dots q_s^{\delta_s}$$

it follows that the products de are positive divisors of mn, and every positive divisor of mn can be written uniquely in this form. Finally, by Theorem 11 again, d (resp. e) is a positive divisor of m (resp. n) and every positive divisor of m (resp. n) appears exactly once among the d's (resp. e's) considered. □

Remark 11. If m and n are relatively prime and $k \mid mn$ then the components $d \mid m$ and $e \mid n$ in Theorem 13 can be described as $d = (k, m)$ and $e = (k, n)$. This follows at once from the proof and Theorem 12. In particular, $k = (k, m)(k, n)$ for all $k \mid mn$. More generally, Theorem 12 easily implies that $(k, mn) = (k, m)(k, n)$ for arbitrary k.

3. Congruences

Definition 6. $a \equiv b \pmod{n}$ if $n \mid a - b$. We say that *a is congruent to b modulo n*.

Example 3. $5 \equiv 0 \pmod{5}$. $-3 \equiv 19 \pmod{11}$.

Proposition 6. *For arbitrary a, b, c, d, m, n we have the following.*

1. $a \equiv a \pmod{n}$.
2. *If* $a \equiv b \pmod{n}$ *then* $b \equiv a \pmod{n}$.
3. *If* $a \equiv b \pmod{n}$ *and* $b \equiv c \pmod{n}$ *then* $a \equiv c \pmod{n}$.
4. *If* $a \equiv b \pmod{n}$ *and* $c \equiv d \pmod{n}$ *then* $a + c \equiv b + d \pmod{n}$.
5. *If* $a \equiv b \pmod{n}$ *and* $c \equiv d \pmod{n}$ *then* $ac \equiv bd \pmod{n}$.

Proof. (1): We need to show that $n \mid a - a$, that is, $n \mid 0$ which is obvious. (2): We need to show that if $n \mid a - b$ then $n \mid b - a$ which is obvious. (3): We need to show that if $n \mid a - b$ and $n \mid b - c$ then $n \mid a - c$. This follows at once from (5) of Proposition 1. (4): We need to show that if $n \mid a - b$ and $n \mid c - d$ then $n \mid (a + c) - (b + d)$. Observe that $(a + c) - (b + d) = (a - b) + (c - d)$. Therefore the statement follows from (5) of Proposition 1. (5): We need to show that if $n \mid a - b$ and $n \mid c - d$ then $n \mid ac - bd$. Observe that $ac - bd = (a - b)c + (c - d)b$. Therefore the statement follows from (6) of Proposition 1. □

Proposition 7. *If $(a, n) = 1$ then $ax \equiv ay \pmod{n}$ implies $x \equiv y \pmod{n}$.*

Proof. We need to show that $n \mid ax - ay$ implies $n \mid x - y$. As $ax - ay = a(x - y)$ and $(a, n) = 1$ the statement follows from Theorem 6. □

Proposition 8. *For arbitrary a and n the congruence*

$$ax \equiv 1 \pmod{n}$$

has a solution if and only if $(a, n) = 1$. Moreover, the solutions x can be given as $x \equiv \bar{a} \pmod{n}$, where $\bar{a}$ denotes any particular solution.

Proof. The given congruence is satisfied if and only if $ax - ny = 1$ holds for some y. By Theorem 3 this equation has a solution x, y if and only if $(a, n) = 1$. If this condition is satisfied then Corollary 2 shows that the solutions are of the form $x = x_0 + kn$ and $y = y_0 + ka$, where $ax_0 - ny_0 = 1$. In particular, putting $\bar{a} := x_0$ we can see that x is admissible if and only if $x \equiv \bar{a} \pmod{n}$. □

Remark 12. Any $\bar{a}$ with the property that $a\bar{a} \equiv 1 \pmod{n}$ is called a *multiplicative inverse* of a modulo n. By Theorem 8 $\bar{a}$ exists if and only if $(a, n) = 1$ and in that case $\bar{a}$ is uniquely determined modulo n. Using $\bar{a}$ we can obtain an alternate proof of Proposition 7: simply multiply both sides of $ax \equiv ay \pmod{n}$ by $\bar{a}$.

Proposition 9. *Let $n_1, n_2, \ldots, n_k$ be pairwise relatively prime and put $n := n_1 n_2 \ldots n_k$. Then for arbitrary x, y the congruences*

$$x \equiv y \pmod{n_i}, \qquad i = 1, 2, \ldots, k$$

hold simultaneously if and only if

$$x \equiv y \pmod{n}.$$

Proof. We need to show that $n_i \mid x - y$ holds for all i if and only if $n \mid x - y$. As the n_i's are pairwise relatively prime, the statement follows at once from Theorem 4. □

Theorem 14 (Chinese Remainder Theorem)**.** *Let $n_1, n_2, \ldots, n_k$ be pairwise relatively prime positive integers and let $a_1, a_2, \ldots, a_k$ be arbitrary. The congruences*

$$x \equiv a_i \pmod{n_i}, \qquad i = 1, 2, \ldots, k$$

can be satisfied simultaneously. Moreover, the solutions x can be given as

$$x \equiv x_0 \pmod{n},$$

where $n := n_1 n_2 \ldots n_k$ and x_0 is any particular solution.

Proof. Let us first show that the congruences $x \equiv a_i \pmod{n_i}$ can be satisfied simultaneously. Let $R_i := \{0, 1, \ldots, n_i - 1\}$ and $R := \{0, 1, \ldots, n - 1\}$. In the light of Theorem 1 and Proposition 6 we can assume that each a_i is taken from R_i. Let $x \in R$ be arbitrary. By Theorem 1 for each i there is a unique $x_i \in R_i$ satisfying $x \equiv x_i \pmod{n_i}$. Putting $f(x) := (x_1, x_2, \ldots, x_k)$ we have defined a function $f : R \to R_1 \times R_2 \times \ldots R_k$. Observe that the domain R and the target $R_1 \times R_2 \times \ldots R_k$ of f are of the same size $n := n_1 n_2 \ldots n_k$. We need to show the surjectivity of f which by the previous remark is equivalent to the injectivity of f. We prove the latter. If $f(x) = f(y)$ for $x, y \in R$ then $x \equiv y \pmod{n_i}$ for all i by Proposition 6, hence $x \equiv y \pmod{n}$ by Proposition 9. However, $-n < x - y < n$, therefore $n \mid x - y$ implies $x = y$. We have now shown that some x_0 satisfies all the congruences $x \equiv a_i \pmod{n_i}$. In particular, Proposition 6 shows that the congruences are equivalent to $x \equiv x_0 \pmod{n_i}$. By Proposition 9 these congruences hold simultaneously if and only if $x \equiv x_0 \pmod{n}$. □

Proposition 10. *If* $(a, n) = 1$ *then* $a^k \equiv 1 \pmod{n}$ *for some* $1 \leq k \leq n$.

Proof. Consider the $n+1$ numbers a^i $(i = 0, 1, \ldots, n)$. By the pigeon-hole principle at least two of them share the same residue modulo n, that is, $a^i \equiv a^j$ for some $0 \leq i < j \leq n$. By applying Proposition 7 i times (or alternately by multiplying both sides by $\bar{a}^i$) we conclude $1 \equiv a^{j-i} \pmod{n}$. Hence the proposition follows upon putting $k := j - i$. □

Definition 7. If $(a, n) = 1$ then the least positive k satisfying $a^k \equiv 1 \pmod{n}$ is denoted $\operatorname{ord}_n(a)$ and is called the *order* of a modulo n.

Theorem 15. *If* $(a, n) = 1$ *and* $k \geq 0$ *then*

$$a^k \equiv 1 \pmod{n} \quad \Longleftrightarrow \quad \operatorname{ord}_n(a) \mid k.$$

Proof. Let $m := \operatorname{ord}_n(a)$ then by Theorem 1 there is a unique decomposition $k = mq + r$, where $0 \leq r < m$. Note that $k \geq 0$ implies $m \geq 0$, therefore

$$a^k = a^{mq+r} = (a^m)^q a^r \equiv 1^m a^r = a^r \pmod{n}.$$

Since $0 \leq r < m$, the right hand side is congruent to 1 mod n if and only if $r = 0$, that is, if and only if $m \mid k$. □

Theorem 16. *If* $(a, n) = 1$ *and* $u > 0$ *then*

$$\operatorname{ord}_n(a^u) = \frac{\operatorname{ord}_n(a)}{(u, \operatorname{ord}_n(a))}.$$

Proof. Let $v := \operatorname{ord}_n(a)$ and $k > 0$ be arbitrary. Clearly, $(a^u)^k = a^{uk}$, therefore Theorem 15 shows that $\operatorname{ord}_n(a^u)$ is the least positive k that satisfies $v \mid uk$. In other words, we are looking for the least positive k occurring in the solution of the equation $uk = vl$. By Theorem 5 the solutions are of the form $k = mv/(u, v)$, $l = mu/(u, v)$, hence the least positive k (corresponding to $m = 1$) equals $v/(u, v)$. □

Definition 8. $\varphi(n)$ is the number of elements in $\{0, 1, \ldots, n-1\}$ coprime with n.

Example 4. $\varphi(1) = 1$. If $n = 10$ then $1, 3, 5, 7$ are the elements in $\{0, 1, \ldots, 9\}$ that are coprime with 10, therefore $\varphi(10) = 4$.

Proposition 11. *If* p *is prime and* $\alpha > 0$ *then* $\varphi(p^\alpha) = (p-1)p^{\alpha-1}$. *In particular,* $\varphi(p) = p - 1$.

Proof. It follows by unique factorization that the elements in $\{0, 1, \ldots, p^\alpha - 1\}$ that are not coprime with p^α are exactly those divisible by p, that is, the numbers pk with $0 \leq k < p^{\alpha-1}$. This shows that $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = (p-1)p^{\alpha-1}$. □

Theorem 17. *Let* $n_1, n_2, \ldots, n_k$ *be pairwise relatively prime positive integers. Then*

$$\varphi(n_1 n_2 \ldots n_k) = \varphi(n_1)\varphi(n_2) \ldots \varphi(n_k).$$

Proof. Let us use the notations in the proof of Theorem 14. The map $f : R \to R_1 \times R_2 \times \ldots R_k$ was shown to be bijective in that proof. In particular, for any subset $S \subseteq R$ the image set $f(S) := \{f(x) \mid x \in S\}$ is of the same size as S. Let us consider $S := \{x \in R \mid (x, n) = 1\}$. We claim that $f(S) = S_1 \times S_2 \times \ldots S_k$, where $S_i := \{x_i \in R_i \mid (x_i, n_i) = 1\}$. Clearly, $|S| = \phi(n)$ and $|S_i| = \varphi(n_i)$, hence the claim implies the theorem:

$$\begin{aligned}\varphi(n_1 n_2 \dots n_k) &= \varphi(n)\\ &= |S|\\ &= |f(S)|\\ &= |S_1 \times S_2 \times \dots S_k|\\ &= |S_1| \cdot |S_2| \cdot \ldots \cdot |S_k|\\ &= \varphi(n_1)\varphi(n_2)\dots\varphi(n_k).\end{aligned}$$

So it suffices to show the claim that $f(S) = S_1 \times S_2 \times \dots S_k$. Using that f is bijective this can be reformulated as: if $x \in R$ and $f(x) = (x_1, x_2, \dots, x_k)$, then $x \in S$ if and only if $x_i \in S_i$ for all i. In other words, we need to show that $(x, n) = 1$ if and only if $(x_i, n_i) = 1$ for all i. Combining the congruence $x \equiv x_i \pmod{n_i}$ (the definition of f) with Proposition 3 we can infer that $(x_i, n_i) = (x, n_i)$. So we are left with proving that $(x, n) = 1$ if and only if $(x, n_i) = 1$ for all i. The "only if" part is obvious, since (x, n_i) is a common divisor of x and n. The "if" part follows immediately from Theorem 7 or Theorem 10. □

Corollary 7. *Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, where $p_1 < p_2 < \dots < p_k$ are distinct primes and the exponents α_i are positive. Then*

$$\varphi(n) = (p_1 - 1)p_1^{\alpha_1 - 1}(p_2 - 1)p_2^{\alpha_2 - 1} \dots (p_k - 1)p_k^{\alpha_k - 1}.$$

Proof. Theorem 17 applied for $n_i := p_i^{\alpha_i}$ gives

$$\varphi(n) = \varphi(n_1)\varphi(n_2)\dots\varphi(n_k),$$

and here $\varphi(n_i) = (p_i - 1)^{\alpha_i - 1}$ by Proposition 11. □

Remark 13. The above formula can be written in the more elegant form

$$\frac{\varphi(n)}{n} = \prod_{p \mid n} \left(1 - \frac{1}{p}\right),$$

where the product runs over the prime divisors of n. The left hand side can be interpreted as the probability of the event E that a random number x taken from $\{0, 1, \dots, n-1\}$ with uniform distribution is relatively prime to n. The right hand side can be interpreted as the product of the probabilities of the events E_p that the same random number x is not divisible by p. Of course we know that event E holds if and only if all the events E_p hold simultaneously. Therefore the above formula is a special case of the probabilistic statement that the events E_p (for p a prime divisor of n) are independent. The proof given above could be modified easily to yield this more general statement, that is, the equation

$$\mathrm{Prob}\Big(\bigwedge_{p \mid n} F_p\Big) = \prod_{p \mid n} \mathrm{Prob}(F_p),$$

where each F_p equals either E_p or the negation of E_p.

Theorem 18 (Euler–Fermat). *If $(a, n) = 1$ then $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Proof. Let $r_1, r_2, \dots, r_{\varphi(n)}$ be the elements in $\{0, 1, \dots, n-1\}$ coprime with n (note that $\varphi(n) \geq 1$). By Theorem 7 the numbers $ar_1, r_2, \dots, ar_{\varphi(n)}$ are also coprime with n. Using Theorem 1 and Proposition 3 we can see that for each i there is some j such that

$$ar_i \equiv r_j \pmod{n}.$$

Different i's yield different j's by Proposition 6, hence the assignment $i \mapsto j$ is injective. As the i's and the j's are taken from the same finite set $\{0, 1, \dots, n-1\}$, the assignment $i \mapsto j$ is a permutation. In other words, the numbers $ar_1, r_2, \dots, ar_{\varphi(n)}$ modulo n are the same as $r_1, r_2, \dots, r_{\varphi(n)}$ in some order. It follows that

$$ar_1 \cdot ar_2 \cdot \ldots \cdot ar_{\varphi(n)} \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(n)} \pmod{n}.$$

By Proposition 7 we can divide both sides by r_1, then by r_2, and so on, finally by $r_{\varphi(n)}$, and in this way we obtain

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

□

Corollary 8. *If $(a, n) = 1$ then $\mathrm{ord}_n(a) \mid \varphi(n)$.*

Proof. This follows at once from Theorems 18 and 15. □

Corollary 9. *If p is prime then $a^p \equiv a \pmod{p}$ for all a.*

Proof. If $p \mid a$ then the statement is obvious. If $p \nmid a$ then $(a, p) = 1$, therefore $a^{\varphi}(p) \equiv 1 \pmod{p}$ by Theorem 18. Here $\varphi(p) = p - 1$, hence in fact $a^{p-1} \equiv 1 \pmod{p}$. Multiplying both sides by a we get $a^p \equiv a \pmod{p}$. □

Theorem 19. *If p is prime then every prime factor of $2^p - 1$ is congruent to 1 modulo p.*

Proof. Let q be a prime factor of $2^p - 1$. Then $2^p \equiv 1 \pmod{q}$ which shows by Theorem 15 that $\mathrm{ord}_q(2) \mid p$. As $\mathrm{ord}_q(2) = 1$ is clearly impossible, we conclude that $\mathrm{ord}_q(2) = p$. By Corollary 8 it follows that $\mathrm{ord}_q(2) \mid \varphi(q)$, where $\mathrm{ord}_q(2) = p$ and $\varphi(q) = q - 1$, hence $p \mid q - 1$. □

Remark 14. Theorem 19 shows that for each prime p there is some prime q congruent to 1 modulo p. As q is larger than p we obtained a new proof of Theorem 8.

Definition 9. Let $a > 1$ be an integer. A positive integer n is called a *pseudoprime to the base a* if n is composite and $a^{n-1} \equiv 1 \pmod{n}$.

Theorem 20 (Cipolla)**.** *There are infinitely many pseudoprimes to each base $a > 1$.*

Proof. Let $p > a^2$ be any prime number. We will show that

$$n := \frac{a^{2p} - 1}{a^2 - 1}$$

is a pseudoprime to the base a. As different p's yield different n's we will have constructed infinitely many pseudoprimes to the base a this way.

First note that

$$\begin{aligned} n &= \frac{a^p - 1}{a - 1} \cdot \frac{a^p + 1}{a + 1} \\ &= (a^{p-1} + a^{p-2} + \cdots + a^2 + a + 1)(a^{p-1} - a^{p-2} \pm \cdots + a^2 - a + 1), \end{aligned}$$

therefore n is clearly composite. For later reference we also note that n is odd as on the right hand side both factors are odd. For a even this is clear while for odd a it follows because a sum of an odd number of odd numbers is always odd. Now observe that $(a^2-1)n = a^{2p}-1$, so $n \mid a^{2p}-1$, therefore

$$a^{2p} \equiv 1 \pmod{n}.$$

If we show that $2p \mid n-1$ then we are done, since raising both sides to the $(n-1)/2p$-th power we can conclude

$$a^{n-1} \equiv 1 \pmod{n}.$$

The relation $2p \mid n-1$ is equivalent to $2 \mid n-1$ and $p \mid n-1$. We have already seen that n is odd, so $2 \mid n-1$. For $p \mid n-1$ observe that by Corollary 9

$$(a^2-1)n = a^{2p}-1 \equiv a^2-1 \pmod{p},$$

since $p > a^2$ implies $(a^2, p) = 1$. On the two sides a^2-1 is coprime with p (since $p > a^2$), therefore by Proposition 7 it follows that

$$n \equiv 1 \pmod{p}.$$

In other words, $p \mid n-1$, and the proof is complete. □

Remark 15. From the proof it follows (taking $a = 2$ and $p = 5$) that $n = 341$ is a pseudoprime to the base 2.

Definition 10. A positive integer n is called a *Carmichael number* if n is composite and satisfies $a^{n-1} \equiv 1 \pmod{n}$ for any integer a coprime with n.

Theorem 21 (Korselt)**.** *Let $n = p_1 p_2 \dots p_k$ where $p_1 < p_2 < \dots < p_k$ are distinct primes and $k > 1$. If $p_i - 1 \mid n-1$ for all i, then n is a Carmichael number.*

Proof. Let a be any integer coprime with n. We need to show that $a^{n-1} \equiv 1 \pmod{n}$. By Proposition9 this holds true if and only if $a^{n-1} \equiv 1 \pmod{p_i}$ for all i. As $(a,n) = 1$ we also have $(a, p_i) = 1$, so $a^{p_i-1} \equiv 1 \pmod{p_i}$ by Theorem 18. We assume that $p_i - 1 \mid n-1$, so raising both sides to the $(n-1)/(p_i-1)$-th power we obtain $a^{n-1} \equiv 1 \pmod{p_i}$ as needed. □

Corollary 10. 561 *is a Carmichael number.*

Proof. The prime decomposition of 561 reads $561 = 3 \cdot 11 \cdot 17$. The prime factors satisfy the hypothesis of Theorem 21, since $3-1 = 2$, $11-1 = 10$, and $17-1 = 16$ are all divisors of $561-1 = 560$. □

Remark 16. It can be shown that the condition in Theorem 21 (observed by Korselt in 1899) characterizes all Carmichael numbers. The proof relies on the fact that if $p > 2$ is a prime then for each $\alpha > 0$ there is an a such that $\mathrm{ord}_{p^\alpha}(a) = \varphi(p^\alpha)$. Such an a is called a *primitive root* mod p^α. Carmichael conjectured in 1912 that there are infinitely many Carmichael numbers. Based on Korselt's criterion, Alford, Granville, and Pomerance managed to prove this conjecture in 1994.

4. Quadratic residues

Definition 11. Let p be an odd prime and let a be coprime with p. We say that a is a *quadratic residue* modulo p if there is an x satisfying the congruence $x^2 \equiv a \pmod{p}$. If there is no such x then we say that a is a *quadratic nonresidue* modulo p.

Theorem 22. *Let p be an odd prime. The set $\{1, 2, \dots, p-1\}$ contains $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic nonresidues modulo p.*

Proof. Consider the sets $S := \{1, 2, \dots, (p-1)/2\}$ and $T := \{1, 2, \dots, p-1\}$. For each $x \in S$ there is a unique $a \in T$ satisfying $x^2 \equiv a \pmod{p}$. The assignment $x \mapsto a$ defines a function $f : S \to T$. The image $f(S)$ of this function consists of the quadratic residues modulo p in T. We claim that f is injective, that is, if $x, y \in S$ satisfy $f(x) = f(y)$ then $x = y$. Indeed, if $f(x) = f(y)$ then $x^2 \equiv y^2 \pmod{p}$, therefore $(x-y)(x+y) = x^2 - y^2 \equiv 0 \pmod{p}$, hence $x - y \equiv \pmod{p}$ or $x + y \equiv 0 \pmod{p}$. The second congruence cannot hold, since $0 < x + y < p$, while the first congruence forces $x = y$, since $-p < x - y < p$. The injectivity of f implies that $f(S)$ is of the same size as S. In other words, there are exactly $(p-1)/2$ quadratic residues modulo p in T. It follows, in addition, that the number of quadratic nonresidues modulo p in T is $p - 1 - (p-1)/2 = (p-1)/2$. □

Definition 12. Let p be an odd prime. The *Legendre symbol* of a modulo p is defined as

$$\left(\frac{a}{p}\right) := \begin{cases} +1, & \text{if } a \text{ is a quadratic residue modulo } p\,; \\ -1, & \text{if } a \text{ is a quadratic nonresidue modulo } p\,; \\ 0, & \text{if } a \text{ is divisible by } p\,. \end{cases}$$

Proposition 12. *Let p be an odd prime. For arbitrary a, b we have the following.*

(1) *If $a \equiv b \pmod{p}$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*

(2) *If $p \nmid b$ then $\left(\frac{a}{p}\right) = \left(\frac{ab^2}{p}\right)$.*

Proof. (1): If either of a, b is divisible by p then both of them are divisible by p, hence the statement is obvious. Otherwise the statement means that the congruence $x^2 \equiv a \pmod{p}$ has a solution if and only if the congruence $x^2 \equiv b \pmod{p}$ has a solution. This is immediate from $a \equiv b \pmod{p}$. (2): If a is divisible by p then the statement is obvious. Otherwise the statement means that the congruence $x^2 \equiv a \pmod{p}$ has a solution if and only if the congruence $x^2 \equiv ab^2 \pmod{p}$ has a solution. If the first congruence has some solution x_0 then $x_1 := x_0 b$ solves the second congruence. If the second congruence has some solution x_1 then $x_0 := x_1 \bar{b}$ solves the first congruence, where $b\bar{b} \equiv 1 \pmod{p}$ (cf. Remark 12). □

Theorem 23 (Euler)**.** *Let p be an odd prime and let a be arbitrary. Then*

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

Proof. We can assume that a is not divisible by p for otherwise the statement is obvious. Let $T := \{1, 2, \dots, p-1\}$. We know by Corollary 2 that for every $x \in T$ there is a unique $y \in T$ satisfying $xy \equiv a \pmod{p}$. In fact, y is the unique element of T congruent to $a\bar{x}$ mod p (see Proposition 8 and Remark 12). If a is a quadratic nonresidue mod p then x and y are always different and therefore T decomposes into a disjoint union of $(p-1)/2$ subsets $\{x,y\}$ each consisting of two elements whose product is congruent to a mod p. As a result, the product of all elements of T is congruent to $a^{\frac{p-1}{2}}$ mod p. If a is a quadratic residue mod p then there is an $x_0 \in T$ such that $a \equiv x_0^2 \pmod{p}$. The congruence $a \equiv x^2 \pmod{p}$ has exactly two solutions in T, namely $x = x_0$ and $x = p - x_0$ (note that these are different because p is odd). This is because $a \equiv x^2 \pmod{p}$ can be written as $(x - x_0)(x + x_0) \equiv \pmod{p}$ which is equivalent to $x \equiv \pm x_0 \pmod{p}$. Therefore unless $x = x_0$ or $x = p - x_0$ the element y satisfying $xy \equiv a \pmod{p}$ is different from x and also from x_0 and $p - x_0$. This shows that T now decomposes into a disjoint union of $(p-3)/2$ subsets $\{x,y\}$ each consisting of two elements whose product is congruent to a mod p plus an additional subset $\{x_0, p - x_0\}$ consisting of two elements whose product is $x_0(p-x_0) \equiv -x_0^2 \equiv -a \pmod{p}$. As a result, the product of all elements of T is congruent to $-a^{\frac{p-1}{2}}$ mod p. With the Legendre symbol notation we can summarize the findings in both cases as

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

In the special case of $a = 1$ this congruence reads

$$(p-1)! \equiv -1 \pmod{p},$$

and therefore we even have

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

Multiplying the two sides by $-\left(\frac{a}{p}\right)$ we obtain

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

□

Corollary 11 (Euler). *Let p be an odd prime. Then*

$$\left(\frac{-1}{p}\right) = \begin{cases} +1, & p \equiv +1 \pmod{4}; \\ -1, & p \equiv -1 \pmod{4}. \end{cases}$$

Proof. By Theorem 23 the two sides are congruent modulo p. As $p > 2$ and both sides are either $+1$ or -1, they are equal. □

Theorem 24 (Wilson's Theorem[1]). *If p is prime then*

$$(p-1)! \equiv -1 \pmod{p}.$$

Proof. This congruence is trivial for $p = 2$ and it was derived in the proof of Theorem 23 for $p > 2$. □

Theorem 25. *Let p be an odd prime. For arbitrary a and b we have*

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

[1] proved by Lagrange

First proof (using Theorem 23). By Theorem23

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}.$$

The two sides are elements of $\{-1, 0, 1\}$, therefore $p > 2$ forces them to be equal. □

Second proof (using Theorem 22). If a or b is divisible by p then both sides of the equation are zero, so the statement holds. Otherwise the statement means that ab is a quadratic residue mod p if and only if a and b are both quadratic residues mod p or both quadratic nonresidues mod p. By Theorem 22 the quadratic resides mod p between 0 and p can be labeled as

$$0 < r_1 < r_2 < \cdots < r_{(p-1)/2} < p,$$

while the quadratic nonresidues mod p between 0 and p can be labeled as

$$0 < s_1 < s_2 < \cdots < s_{(p-1)/2} < p.$$

It suffices to show that $r_i r_j$ is always a quadratic residue, $r_i s_j$ is always a quadratic nonresidue, and $s_i s_j$ is always a quadratic residue.

It is clear that $r_i r_j$ is always a quadratic residue, because there are x_i and x_j such that $x_i^2 \equiv r_i \pmod{p}$ and $x_j^2 \equiv r_j \pmod{p}$, and then $x := x_i x_j$ solves the conruence $x^2 \equiv r_i r_j \pmod{p}$. Now fix i and consider the products $r_i r_j$ and $r_i s_j$. These are pairwise incongruent mod p by Proposition 7, therefore by Theorem 22 exactly $(p-1)/2$ of them are quadratic residues mod p. As the $r_i r_j$'s are already known to be quadratic residues mod p, none of the $r_i s_j$'s can be quadratic residues mod p. In other words, $r_i s_j$ is always a quadratic nonresidue. Now fix j and consider the products $r_i s_j$ and $s_i s_j$. These are pairwise incongruent mod p by Proposition 7, therefore by Theorem 22 exactly $(p-1)/2$ of them are quadratic nonresidues mod p. As the $r_i s_j$'s are already known to be quadratic nonresidues mod p, none of the $s_i s_j$'s can be quadratic nonresidues mod p. In other words, $s_i s_j$ is always a quadratic residue. □

Theorem 26 (Gauss's Lemma). *Let p be an odd prime and let a be coprime with p. Let s denote the number of elements k of $\{1, 2, \ldots, (p-1)/2\}$ for which ak is congruent modulo p to some element of $\{-1, -2, \ldots, -(p-1)/2\}$. Then*

$$\left(\frac{a}{p}\right) = (-1)^s.$$

Proof. Let us use the notation $S := \{1, 2, \ldots, (p-1)/2\}$. If k is an arbitrary element of S then ak is coprime with p, hence $ak \equiv \varepsilon_k m_k$ for some $\varepsilon_k \in \{\pm 1\}$ and some $m_k \in S$. Note that ε_k and m_k are uniquely determined by a and k, therefore s is the number of times -1 occurs in the sequence $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{(p-1)/2}$. We claim that $m_1, m_2, \ldots, m_{(p-1)/2}$ are all different. Indeed, if $m_i = m_j$ then either $ai - aj$ or $ai + aj$ is divisible by p, whence by Theorem 9 either $i - j$ or $i + j$ is divisible by p. As $-p < i - j < p$ and $0 < i + j < p$, this forces $i = j$. The m_k's are elements of S, hence in fact they are all the elements of S in some order. It follows that

$$a^{(p-1)/2} \prod_{k \in S} k = \prod_{k \in S} (ak) \equiv \prod_{k \in S} (\varepsilon_k m_k) = \prod_{k \in S} \varepsilon_k \prod_{k \in S} m_k = \prod_{k \in S} \varepsilon_k \prod_{k \in S} k \pmod{p}.$$

Using Proposition 7 for the two sides it follows that

$$a^{(p-1)/2} \equiv \prod_{k \in S} \varepsilon_k = (-1)^s \pmod{p}.$$

Combining with Theorem 23 we obtain

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

As $p > 2$ and both sides are either $+1$ or -1, they are equal. □

Theorem 27. *For $a > 0$ and $(r, 2a) = 1$ put*

$$s_a(r) := \sum_{1\leq m\leq a/2} \left(\left\lfloor\frac{mr}{a}\right\rfloor - \left\lfloor\frac{mr}{a} - \frac{r}{2a}\right\rfloor\right).$$

For all primes p satisfying $p \equiv \pm r \pmod{4a}$ we have

$$\left(\frac{a}{p}\right) = (-1)^{s_a(r)}.$$

Proof. Clearly, $(p, 2a) = (r, 2a) = 1$, therefore p is an odd prime coprime with a. We shall use the notation of the proof of Theorem 26.

We prove first that $s = s_a(p)$. Let us dissect the interval $(0, p/2]$ into a subintervals of equal length:

$$I_n := \left(\frac{(n-1)p}{2a}, \frac{np}{2a}\right], \qquad n = 1, 2, \ldots, a.$$

Each element $k \in S$ lies in exactly one of these intervals. If $k \in S \cap I_n$ then

$$\frac{(n-1)}{2}p \;<\; ak \;\leq\; \frac{n}{2}p.$$

For n odd the left hand side is an integer divisible by p, so $\varepsilon_k = +1$ and $m_k = ak - \frac{(n-1)}{2}p \in S$. For n even the right hand side is an integer divisible by p, so $\varepsilon_k = -1$ and $m_k = \frac{n}{2}p - ak \in S$. This shows that $\varepsilon_k = -1$ if and only if n is even, therefore

$$s = \sum_{1\leq m\leq a/2} |S \cap I_{2m}|.$$

Using the notation

$$J_n := \left(0, \frac{np}{2a}\right], \qquad n = 1, 2, \ldots, a$$

we can see that I_{2m} is just the set-theoretic difference of J_{2m} and its subset J_{2m-1}, hence

$$|S \cap I_{2m}| = |S \cap J_{2m}| - |S \cap J_{2m-1}|.$$

Clearly,

$$|S \cap J_n| = \left\lfloor\frac{np}{2a}\right\rfloor, \qquad n = 1, 2, \ldots, a,$$

therefore

$$|S \cap I_{2m}| = |S \cap J_{2m}| - |S \cap J_{2m-1}| = \left(\left\lfloor\frac{mp}{a}\right\rfloor - \left\lfloor\frac{mp}{a} - \frac{p}{2a}\right\rfloor\right).$$

This shows that

$$s = \sum_{1\leq m\leq a/2} |S \cap I_{2m}| = \sum_{1\leq m\leq a/2} \left(\left\lfloor\frac{mp}{a}\right\rfloor - \left\lfloor\frac{mp}{a} - \frac{p}{2a}\right\rfloor\right) = s_a(p).$$

By Theorem 26 it follows that

$$\left(\frac{a}{p}\right) = (-1)^{s_a(p)}.$$

To complete the proof we shall show that $s_a(p) \equiv s_a(r) \pmod 2$. We know that $p = 4aq + r$ or $p = 4aq - r$ for some q. Let n be an arbitrary integer not divisible by $2a$, then np is also not divisible by $2a$ as follows from Theorem 6 and $(p, 2a) = 1$. Therefore

$$p = 4aq + r \quad \Longrightarrow \quad \left\lfloor \frac{np}{2a} \right\rfloor = 2nq + \left\lfloor \frac{mr}{a} \right\rfloor \equiv \left\lfloor \frac{mr}{a} \right\rfloor \pmod 2,$$

while

$$p = 4aq - r \quad \Longrightarrow \quad \left\lfloor \frac{np}{2a} \right\rfloor = 2nq - 1 - \left\lfloor \frac{mr}{a} \right\rfloor \equiv 1 + \left\lfloor \frac{mr}{a} \right\rfloor \pmod 2.$$

If $0 < m < a$ then in either case we obtain, by subtracting the relevant congruences for $n = 2m$ and $n = 2m - 1$,

$$\left\lfloor \frac{mp}{a} \right\rfloor - \left\lfloor \frac{mp}{a} - \frac{p}{2a} \right\rfloor \equiv \left\lfloor \frac{mr}{a} \right\rfloor - \left\lfloor \frac{mr}{a} - \frac{r}{2a} \right\rfloor \pmod 2.$$

By summing up these congruences for $1 \le m \le a/2$ we obtain

$$s_a(p) \equiv s_a(r) \pmod 2.$$

Finally,

$$\left(\frac{a}{p}\right) = (-1)^{s_a(p)} = (-1)^{s_a(r)}.$$

□

Corollary 12 (Lagrange)**.** *Let p be an odd prime. Then*

$$\left(\frac{2}{p}\right) = \begin{cases} +1, & p \equiv \pm 1 \pmod 8; \\ -1, & p \equiv \pm 3 \pmod 8). \end{cases}$$

and

$$\left(\frac{-2}{p}\right) = \begin{cases} +1, & p \equiv +1, +3 \pmod 8; \\ -1, & p \equiv -1, -3 \pmod 8). \end{cases}$$

Proof. The first identity follows immediately from Theorem 27 upon remarking that

$$s_2(1) = \left\lfloor \frac{1}{2} \right\rfloor - \left\lfloor \frac{1}{2} - \frac{1}{4} \right\rfloor = 0 \quad \text{and} \quad s_2(3) = \left\lfloor \frac{3}{2} \right\rfloor - \left\lfloor \frac{3}{2} - \frac{3}{4} \right\rfloor = 1.$$

The second identity follows from the first identity combined with Theorem 25 and Corollary 11. □

Theorem 28 (Gauss)**.** *Let a be a positive integer. If p and q are odd primes such that $p \equiv \pm q \pmod{4a}$ then*

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$

Proof. The statement follows immediately from Theorem 27:

$$\left(\frac{a}{p}\right) = (-1)^{s_a(q)} = \left(\frac{a}{q}\right).$$

□

Theorem 29 (Gauss)**.** *If p and q are distinct odd prime numbers then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Proof. We assume first that $p\not\equiv q \pmod 4$. Then $p+q$ is some positive integer divisible by 4 and coprime with p and q. If $4a$ denotes this positive integer then clearly $p\equiv -q \pmod{4a}$, hence by Proposition 12 and Theorem 28 we have

$$\left(\frac{q}{p}\right)=\left(\frac{p+q}{p}\right)=\left(\frac{4a}{p}\right)=\left(\frac{a}{p}\right)=\left(\frac{a}{q}\right)=\left(\frac{4a}{q}\right)=\left(\frac{p+q}{q}\right)=\left(\frac{p}{q}\right).$$

Multiplying both sides by $\left(\frac{p}{q}\right)$ we obtain

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=+1.$$

We assume now that $p\equiv q \pmod 4$. Without loss of generality $p<q$ and then $q-p$ is some positive integer divisible by 4 and coprime with p and q. If $4a$ denotes this positive integer then clearly $p\equiv q \pmod{4a}$, hence by Proposition 12 and Theorem 28 we have

$$\left(\frac{q}{p}\right)=\left(\frac{q-p}{p}\right)=\left(\frac{4a}{p}\right)=\left(\frac{a}{p}\right)=\left(\frac{a}{q}\right)=\left(\frac{4a}{q}\right)=\left(\frac{q-p}{q}\right)=\left(\frac{-p}{q}\right).$$

Applying Theorem 25 for the right hand side and then multiplying both sides by $\left(\frac{p}{q}\right)$ we obtain

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right)\left(\frac{p}{q}\right)\left(\frac{-1}{q}\right)=\left(\frac{-1}{q}\right).$$

Finally by Corollary 11 we conclude that

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=\begin{cases}+1, & p\equiv q\equiv +1 \pmod 4;\\ -1, & p\equiv q\equiv -1 \pmod 4.\end{cases}$$

In both cases we arrived at the conclusion of the theorem, since the exponent $\frac{p-1}{2}\frac{q-1}{2}$ is odd if and only if $p\equiv q\equiv -1 \pmod 4$. □