Further linear algebra. Chapter I. Integers.

Andrei Yafaev

Number theory is the theory of $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$.

1 Euclid's algorithm, Bézout's identity and the greatest common divisor.

- We say that $a \in \mathbb{Z}$ *divides* $b \in \mathbb{Z}$ iff there exists $c \in \mathbb{Z}$ such that $b = ac$. We write $a|b$.

- A *common divisor* of a and b is an integer d that divides both a and b.

- Suppose for simplicity that a and b strictly positive. The *greatest common divisor* (sometimes called the *highest common factor*) of a and b is a common divisor d of a and b such that any other common divisor is smaller than d. This is written $d = \gcd(a, b)$.

  Every $a \in \mathbb{Z}$ is a divisor of 0, since $0 = 0 \times a$, therefore it makes sense to define $\gcd(a, 0) = a$ if $a > 0$. However $\gcd(0, 0)$ does not exist as any integer is a common factor of 0 and 0.

The following obvious remark : any divisor of $a \geq 0$ is *smaller or equal* to a, is often used in the proofs.

Let $a \geq b > 0$ be two integers. When a is not divisible by b, one can still divide with the *remainder*. For example:

$$a = 5, b = 2, a = 2b + 1$$

$$a = 20, b = 3, a = 6b + 2$$

etc..

This leads to the following (fundamental) theorem.

Theorem 1.1 (Euclidean divison) *Let $a \geq b > 0$ be two integers. There exists a* UNIQUE *pair of integers (q, r) satisfying*

$$a = qb + r$$

and $0 \leq r < b$.

Proof. Two things need to be proved : the existence of (q, r) and its uniqueness.

Let us prove the *existence*.

Consider the set

$$S = \{x, x \text{ integer } \geq 0 : a - xb \geq 0\}$$

The set S is not empty : 1 belongs to S. The set S is bounded : any element x of S satisfies $x \leq \frac{a}{b}$. Therefore, S being a bounded set of positive integers, S is finite and hence contains a maximal element. Let q be this maximal element and let $r := a - qb$.

We need to prove that $0 \leq r < b$. By definition $r \geq 0$ (it belongs to S). To prove that $r < b$, let us argue by contradiction. Suppose that $r \geq b$. As $r = a - qb$, we get

$$a - (q + 1)b \geq 0$$

This means that $q + 1 \in S$ but $q + 1 > q$. This contradicts the *maximality* of q. Therefore $r < b$ and the existence is proved.

Let us now prove the *uniqueness*.

Again we argue by contradiction. Suppose that there exists a pair (q', r') satisfying $a = q'b + r'$ with $0 \leq r' < b$ and such that $q' \neq q$. By subtracting the inequality $0 \leq r < b$ to this inequality, we get $-b < r' - r < b$ i.e.

$$|r - r'| < b$$

Now by subtracting $a = q'b + r'$ to $a = qb + r$ and taking the modulus, we get

$$|r - r'| = |q - q'|b$$

By assumption $q \neq q'$, hence $|q' - q| \geq 1$ and we get the inequality

$$|r - r'| \geq b$$

The two inequalities satisfied by $r - r'$ contradict each other, hence $q = q'$. Now $|r - r'| = |q - q'|b = 0$, hence $r = r'$. The uniqueness is proved. $\square$

Theorem 1.2 *Let $a \geq b > 0$ be two integers and (q, r) such that*

$$a = bq + r, \ 0 \leq r < b$$

Then

$$\gcd(a, b) = \gcd(b, r).$$

Proof. Let $A := \gcd(a, b)$ and $B := \gcd(b, r)$. As $r = a - bq$ and A divides a and b, A divides r. Therefore A is a common factor of b and r. As B is the highest common divisor of b and r, $A \leq B$.

In exactly the same way, one proves (left to the reader), that $B \leq A$ and therefore $A = B$. $\square$

This leads to the following algorithm (the so-called **Euclid's algorithm**).

Let $a \geq b > 0$ be two integers. We wish to calculate $\gcd(a, b)$.

The method is this: Set $r_1 = a$ and $r_2 = b$. We have

$$r_1 = r_2 q_1 + r_3$$

with, by he above proposition, $\gcd(a, b) = \gcd(r_1, r_2) = \gcd(r_2, r_3)$ with $0 \leq r_3 < r_2$.

- If $r_3 = 0$, then $\gcd(r_2, r_3) = r_2$ and we are done.
- If $r_3 \neq 0$, then divide r_2 by r_3:

  $$r_2 = r_3 q_2 + r_4$$

  with $0 \leq r_4 < r_3$. Again, if $r_4 = 0$, then $\gcd(a, b) = r_3$, otherwise carry on...

  This was one constructs a sequence:

  $$r_i = r_{i+1} q_i + r_{i+2}$$

  where $0 \leq r_{i+2} < r_{i+1}$.

  Notice that r_{i+2} goes **strictly down** hence one **must** at some point find $r_{i+2} = 0$ and then $\gcd(a, b) = r_{i+1}$.

Remark 1.3 *When performing Euclid's algorithm, be very careful not to divide q_i by r_i. This is a mistake very easy to make.*

Example 1.4 *Take $a = 27$ and $b = 7$. We have*

$$\begin{aligned} 27 &= 3 \times 7 + 6 r_1 = 27,\ r_2 = 7, r_3 = 6 \\ 7 &= 1 \times 6 + 1,\ r_3 = 6, r_4 = 1 \\ 6 &= 6 \times 1 + 0\ r_5 = 0 \end{aligned}$$

Therefore

$$\gcd(27, 7) = \gcd(7, 6) = \gcd(6, 1) = \gcd(1, 0) = 1.$$

Another example:

$$\begin{aligned} 555 &= 155 \cdot 3 + 90 \\ 155 &= 90 \cdot 1 + 65 \\ 90 &= 65 \cdot 1 + 25 \\ 65 &= 25 \cdot 2 + 15 \\ 15 &= 10 \cdot 1 + 5 \\ 10 &= 5 \cdot 2 + 0 \\ \gcd(555, 155) &= 5 \end{aligned}$$

Euclid's algorithm is and **algorithm** meaning that no matter what the initial data is, it will yield a gcd in a finite number of steps.

It is easy to implement on a computer. Suppose that you have some standard computer language (Basic, Pascal, Fortran,...) and that it has an instruction $r := a \bmod b$ which returns the remainder of the Euclidean division of a by b.

The implementation of the algorithm would be something like this:

```
Procedure gcd(a, b)
If  a < b  then
            Swap(a, b)
While b ≠ 0
Begin
            r := a mod b
            a := b
            b := r
End
Return a
End
```

The following lemma is very important for what will follow. It is essentially 'the Euclid's algorithm' run backwards.

Theorem 1.5 (Bézout's Identity) *As usual, let $a \geq b > 0$ be integers. Let $d = \gcd(a, b)$. Then there are integers $h, k \in \mathbb{Z}$ such that*

$$d = ha + kb.$$

Note that in this lemma, the integers h and k *are not positive*, in fact *exactly* one of them is negative or zero. Prove it !

Proof. Consider the sequence given by Euclid's algorithm:

$$r_i = r_{i+1}q_i + r_{i+2}$$

where $0 \leq r_{i+2} < r_{i+1}$ with $r_1 = a, r_2 = b$.

We will show that each r_i can be expressed as $h_i a + k_i b$ with $h_i, k_i \in \mathbb{Z}$. In particular, as by Euclid's algorithm, $\gcd(a, b)$ is some r_i, the result will follow.

This is certainly true for $i = 1, 2$ since $r_1 = 1\times a + 0\times b$ and $r_2 = 0\times a + 1\times b$.

For the inductive step, assume it is the case for r_{i-1} and r_{i-2}, i.e.

$$r_{i-1} = ha + bk, \quad r_{i-2} = h'a + k'b.$$

We have

$$r_{i-2} = q_{i-2}r_{i-1} + r_i.$$

Therefore

$$r_i = h'a + k'b - q_{i-2}(ha + kb) = (h' - q_{i-2}h)a + (k' - q_{i-2}k)b.$$

$\square$

Example 1.6 *Again we take $a = 27$ and $b = 7$.*

$$\begin{aligned} 27 &= 3 \times 7 + 6 \\ 7 &= 1 \times 6 + 1 \\ 6 &= 6 \times 1 + 0. \end{aligned}$$

Therefore

$$\begin{aligned} 1 &= 7 - 1 \times 6 \\ &= 7 - 1 \times (27 - 3 \times 7) \\ &= 4 \times 7 - 1 \times 27. \end{aligned}$$

So we take $h = -1$ and $k = 4$.

Another example

Example 1.7 *Take* $a = 819$ *and* $b = 165$.

$$\begin{aligned} 819 &= 165 \times 4 + 159 \\ 165 &= 159 \times 1 + 6 \\ 6 &= 3 \times 2 \end{aligned}$$

Therefore

$$\begin{aligned} 3 &= 159 + (-26)6 = \\ (819 + 165(-4)) + (-26)(165 + 159(-1)) &= \\ 819 + 165(-30) + 159(26) &= \\ 819 + 165(-30) + (819 + 165(-4))(26) &= \\ 819(27) + 165(-134) & \end{aligned}$$

So we take $h = 27$ *and* $k = -134$.

Définition 1.1 *Two integers* a *and* b *are* **coprime** *if* $\gcd(a, b) = 1$.

Proposition 1.8 a *and* b *are coprime if and only if there exist integers* k *and* h *such that* $ha + kb = 1$.

Proof. If a and b are coprime, then it's just the Bézout's identity. Suppose that there exist integers k and h such that $ha + kb = 1$. Let $d = \gcd(a, b)$. Then d divides $ha + kb$, hence d divides 1, hence $d = 1$. □

For example, for any positive integer k, $6 \cdot (7k + 6) + (-7) \cdot (6k + 5) = 1$, hence $\gcd(7k + 6, 6k + 5) = 1$.

One has the following properties of the gcd.

- if $ha + kb = m$ for some integers h, k, then $\gcd(a, b)$ divides m.
- $\gcd(ca, cb) = c \gcd(a, b)$
- If d divides a and b, then $\gcd(a/d, b/d) = \gcd(a, b)/d$. In particular, if $d = \gcd(a, b)$, then $\gcd(a/d, a/b) = 1$.

The first property is obvious. For the second, write the Bézout's identity $ha + kb = d$ with $d = \gcd(a, b)$. Hence $cd = hac + kbc$ and hence any common divisor of ac and bc divides cd and hence smaller or equal to cd. In addition, cd divides ac and bc hence $\gcd(ca, cb) = cd$. The next property follows from this.

We now apply the Euclid's algorithm and Bézout's identity to the solution of *linear diophantine equations*.

Let a, b, c be three positive integers. A linear diophantine equation (in two variables) is the equation

$$ax + by = c$$

A solution is a pair (x, y) of integers (not necessarily positive) that satisfy this relation.

Such an equation may or may not have solutions. For example, consider $2x+4y = 5$. Quite clearly, if there was a solution, then 2 will divide the right hand side, which is 5. This is not the case, therefore, this equation does not have a solution.

On the other hand, the equation $2x + 4y = 6$ has many solutions : $(1, 1), (5, -1), ...$ This suggests that the existence of solutions depends on whether or not c is divisible by the $\gcd(a, b)$ and that if such is the case, there are many solutions to the equation. This indeed is the case, as shown in the following theorem.

Theorem 1.9 *Suppose that $a|bc$ and a and b are coprime. Then $a|c$.*

In particular, if p is a prime and $p|ab$ then $p|a$ or $p|b$.

Proof. a and b are coprime, hence there exist h and k such that $ha+kb = 1$. Multiply by c and get $c = hac + kbc$. a divides ac and bc, hence a divides the right hand side. It follows that a divides c.

The second statement follows trivially as if p does not divide a, then a and p are coprime. $\square$

Theorem 1.10 (Solution to linear diophantine equations) *Let a, b, c be three positive integers, let $d := \gcd(a, b)$ and consider the equation*

$$ax + by = c$$

1. *This equation has a solution if and only if d divides c*

2. *Suppose that $d|c$ and let (x_0, y_0) be a solution. The set of all solutions is $(x_0 + n\frac{b}{d}, y_0 - n\frac{a}{d})$ where n runs through the set of all integers (positive and negative).*

Proof. For the 'if' part : Suppose there is a solution (x, y). Then d divides $ax + by$. But, as $ax + by = c$, d divides c.

For the 'only if' part : Suppose that d divides c and write $c = dm$ for some integer m. By Bézout's lemma there exist integers h, k such that

$$d = ha + kb$$

Multiply this relation by m and get

$$c = dm = (mh)a + (mk)b$$

This shows that $(x_0 = mh, y_0 = mk)$ is a solution to the equation. That finishes the 'only if' part.

Let us now suppose that the equation has a solution (in particular d divides c) (x_0, y_0). Let (x, y) be any other solution. Subtract $ax + by = c$ from $ax_0 + by_0 = c$ to get

$$a(x_0 - x) + b(y_0 - y) = 0$$

Divide by d to get

$$\frac{a}{d}(x_0 - x) = -\frac{b}{d}(y_0 - y)$$

This relation shows that $\frac{a}{d}$ divides $\frac{b}{d}(y_0 - y)$ but the integers $\frac{a}{d}$ and $\frac{b}{d}$ are coprime hence $\frac{a}{d}$ divides $y_0 - y$ (by 1.9)

Therefore, there exists an integer n such that

$$y = y_0 - n\frac{a}{d}$$

Now plug this into the equality $\frac{a}{d}(x_0 - x) = -\frac{b}{d}(y_0 - y)$ to get that

$$x = x_0 + n\frac{b}{d}$$

□

The proof of this theorem gives a *procedure* for finding solutions, it is as follows:

1. Calculate $d = \gcd(a, b)$. If d does not divide c, then there are no solutions and you're done. If d divides c, $c = md$ then there are solutions.

2. Run Euclid's algorithm backwards to find h, k such that $d = ha + kb$. Then $(x_0 = mh, y_0 = mk)$ is a solution.

3. All solutions are
$$(x_0 + n\frac{b}{d}, y_0 - n\frac{a}{d})$$
where n runs through all integers.

Example 1.11 *Take $a = 27, b = 7, c = 5$. We have found that* $\gcd(a, b) = 1$ *(in particular there will be solutions with any c) and that $1 = 4 \times 7 - 1 \times 27$ hence $h = -1$ and $k = 4$.*

Our procedure gives a particular solution : $(-5, 20)$ and the general one $(-5 + 7n, 20 - 27n)$.

Take $a = 666, b = 153, c = 43$. We have found that $\gcd(a, b) = 9$*, it does not divide 43, hence no solutions.*

Take $c = 45 = 5 \times 9$. There will be solutions. We had $9 = 3 \times 666 - 13 \times 153$. A particular solution is $(15, -65)$ and the general one is $(15 + 17n, -65 - 74n)$.

(in particular there will be solutions with any c) and that $1 = 4 \times 7 - 1 \times 27$ hence $h = -1$ and $k = 4$.

Our procedure gives a particular solution : $(-5, 20)$ and the general one is $(-5 + 7n, 20 - 27n)$.

2 Factorisation into primes.

Définition 2.1 *An integer $p \geq 2$ is* prime *iff the only divisors of p are 1 and p.*

Lemma 2.1 *If $p | a_1 \cdots a_n$ then there exists $1 \leq i \leq n$ such that $p | a_i$.*

Proof. One proceeds by induction. True for $i = 1, 2$ so suppose true for $n - 1$ and suppose that $p | a_1 \cdots a_n$. Let $A = a_1 \cdots a_{n-1}$ and $B = a_n$ then $p | AB$ implies $p | A$ or $p | B$. In the latter case we are done and in the former case the inductive hypothesis implies that $p | a_i$ for some $1 \leq i \leq n - 1$. $\square$

Theorem 2.2 (Unique Factorisation Theorem) *If $a \geq 2$ is an integer then there are primes $p_i > 0$ such that*

$$a = p_1 p_2 \cdots p_s.$$

Moreover this factorisation is unique *in the sense that if*

$$a = q_1 q_2 \cdots q_t$$

for primes $q_j > 0$ then

$$s = t$$

and

$$\{p_1, \ldots, p_s\} = \{q_1, \ldots, q_s\}$$

(equality of sets) In other words, the p_is and the q_is are the same prime numbers up to reodering.

Proof. For existence suppose the result does not hold. Then there an integer which can not be written as a product of primes. Among all those integers, there is a smallest one (the integers under consideration are greater than two !). Let a be this smallest integer which is not a product of primes. Certainly a is not prime so $a = bc$ with $1 < b, c < a$. As b abd c are stricly smaller than a, they are products of primes. Write

$$b = p_1 \cdots p_k$$

and

$$c = p_{k+1} \cdots p_l$$

hence

$$a = p_1 \cdots p_l,$$

This contradicts the definition of a hence the factorisation exists.

For uniqueness suppose that we have an example where there are two distinct factorisations. Again we can choose a *smallest* integer with two diffrent factorisations

$$a = p_1 \cdots p_s = q_1 \cdots q_t.$$

Then $p_1 | q_1 \cdots q_t$ so by lemma 2.1 we have $p_1 | q_j$ for some $1 \leq j \leq t$ then since p_1 and q_j are primes we have $p_1 = q_j$. But then dividing a by p_1 we have a smaller integer with two distinct factorisations, a contradiction. $\square$

Remark 2.3 *Of course, the primes in the factorisation* $a = p_1 \cdots p_s$ *need not be distinct. For example :* $4 = 2^2$*, here* $p_1 = p_2 = 2$*. Similarly* $8 = 2^3, p_1 = p_2 = p_3 = 3$*. Also* $12 = 3 \times 2^2, p_1 = 3, p_2 = p_3 = 2$

In fact we have that for any integer $a \geq 2$*, there exist* s distinct *primes* $p_1, \ldots, p_s$ *and* t *integers* $e_i \geq 1$ *such that*

$$a = p_1^{e_1} \cdots p_s^{e_t}$$

Examples of factorisations:

$$\begin{aligned} 1000 &= 2^3 \times 5^3 \\ 144 &= 2^4 \times 3^2 \\ 975 &= 2^3 \times 5^3 \end{aligned}$$

Factoring a given integer is hard as there is no procedure like Euclidean algorithm. One unsually does it by trial and error. The following trivial lemma helps.

Lemma 2.4 (Square root test) *Let* n *be a composite (not prime) integer. Then* n *has a prime divisor* $\leq \sqrt{n}$*.*

Proof. Write $n = ab$ with $1 < a, b < n$. Suppose that $a \geq \sqrt{n}$, then $n = ab \geq \sqrt{n} b$ hence $b \leq \sqrt{n}$ and therefore any prime divisor of b is $\leq \sqrt{n}$. $\square$

For example, suppose you were to factor 3372. Clearly it's divisible by $2 : 3372 = 2 \times 1686$. Now, 1686 is again divisible by two : $1686 = 2 \times 843$ and $3372 = 2^2 \times 843$. Now we notice that 3 divides $843 = 3 \times 281$. Now the primes $< \sqrt{281}$ are $2, 3, 5, 7, 11, 13$ and 281 is not divisible by any of these. Hence 281 is prime and we get a factorisation:

$$3372 = 2^2 \cdot 3 \cdot 281$$

How many primes there are ? Here is the answer.

Theorem 2.5 (Euclid's Theorem) *There exist infinitely many primes.*

Proof. Suppose not, let $p_1, \dots p_n$ be all the primes there are. Consider $Q = p_1 p_2 \cdots p_n + 1$. Since Q has a prime factorisation, there is a prime p that divides Q. This prime p has to belong to our list, after reordering we can assume that $p = p_1$. Then p_1 divides $Q - p_1 \cdots p_n = 1$ which is not possible because p_1 is prime. $\square$

The idea we used here is this : suppose the set of all primes is finite, we *construct* an integer that is not divisible by any of the primes from this set. This is a contradiction.

Can we use the same idea to prove that there are infinitely many primes of a certain form? In some cases yes.

Quite clearly Euclid's theorem shows that there are infinitely many *odd* primes since the only even prime is 2. Put in another way, it shows that there are infinitely many primes of the form $2k+1$.

Let's look at primes of the form $4k+3$. Are there infinitely many of them ?

Suppose there are finitely many and list them $p_1, \dots, p_r$. Note that $p_1 = 3$. Consider $Q = 4p_2 \cdots p_r + 3$ (note that we started at p_2 !!!).

The integer Q is clearly not divisible by 3 (otherwise 3 would divide $p_2 \cdots p_r$ and $p_i \neq 3$ for all $i > 1$).

None of the p_i, $i > 2$ divides Q. Indeed suppose some p_i, $i > 2$ divides Q. Then

$$4p_2 \cdots p_r + 3 = p_i k$$

which shows that p_i divides 3 which is not the case.

To get a contradiction, we need to prove that Q is divisible by a prime of the form $4k+3$, for it will have necessarily be one of the p_is and they do not divide Q.

Thisis precisely what we are proving.

Lemma 2.6 *Every integer of the form $4k+3$ has a prime factor of the form $4k+3$.*

Proof. Let $N = 4k+3$.

The smallest positive integer of this form is 3 which is prime, hence the property holds for 3.

Suppose that the property holds for all integers $< N$ of the form $4k+3$. If N is prime, then take for the factor N itself.

We can and do assume that N is composite. Write $N = N_1 N_2$ with $1 < N_i < N$. As N is odd, N_1 and N_2 are odd. Any odd number is of the form $4k+1$ or $4k+3$.

Suppose $N_1 = 4a+1$ and $N_2 = 4b+1$. Then $N = N_1 N_2 = (4a+1)(4b+1) = 4(4ab+a+b)+1$ is of the form $4k+1$ which contradicts the fact that N is of the form $4k+3$. Hence one of the N_is, N_1 say has a prime factor of the form $4k+3$. As $N_1 < N$, by induction assumption, N_1 and hence N has a prime factor of the form $4k+3$. This finishes the proof. $\square$

Note that the proof does not work if you try to prove that there are infinitely many primes of the form $4k+1$. This is where it fails. The first prime of this form is $5 = 4 \times 1 + 1$ but when you try to construct your Q, you get $Q = 4 \times 5 + 1 = 21 = 3 \times 7$. The divisors of Q are of the form $4k+3$, not $4k+1$....

In other words, the method fails because the divisors of Q can have no divisor of the form $4k+1$.

It is however true that there are infinitely many primes of the form $4k+1$, in fact, there is the following spectacular theorem :

Theorem 2.7 (Dirichlet's theorem on primes in arithmetic progressions) *Let a and d be two coprime integers. There exist infinitely many primes of the form $a+kd$.*

The proof of this theorem is well beyond the scope of this course.

2.1 Congruences.

We define $a \equiv b \mod m$ iff $m|(a-b)$ in other words iff there exists an integer $k \in \mathbb{Z}$ such that $a = b + km$.

We say a is *congruent* to b modulo m.

The *congruency class* of a is the set of numbers congruent to a modulo m. This is written $[a]$. In other words

$$[a] = \{a + km : k \in \mathbb{Z}\}$$

Every integer is congruent to one of the numbers $0, 1, \ldots, m-1$ (can be seen using Euclidean division), so the set of all congruency classes is

$$\mathbb{Z}/m\mathbb{Z} = \{[0], \ldots, [m-1]\}$$

Ex. Take $m = 3$, them $[8] = [5] = [2] = [-1] = [-4] = ...$

For an integer k, $4k + 1 \equiv 1 \bmod 4$, $4k + 3 \equiv 3 \bmod 4$ and $4k \equiv 0 \bmod 4$.

An integer is *even* if and only if it is zero mod 2. An integer is *odd* if and only if it is one mod 2.

Let $a \geq b$ be two positive integers and let (q, r) be such that $a = bq + r$. Then $a \equiv r \mod b$. It may help to think of congruences as the remainders of the Euclidean division.

Another trivial but useful observation is that if $a \equiv b \bmod m$ and d divides a, b and m, then $\frac{a}{d} \equiv \frac{b}{d} \bmod \frac{m}{d}$.

Proposition 2.8 *If $a \equiv b \mod m$ then $b \equiv a \bmod m$.*
If $a \equiv a' \mod m$ and $b \equiv b' \mod m$ then $a + b \equiv a' + b' \mod m$ and $ab \equiv a'b' \mod m$.

Proof. trivial $\square$

We can rewrite this proposition by simply saying:

$$[a] + [b] = [a + b] \text{ and } [a][b] = [ab]$$

The proposition says that these operations $+$ and $\times$ are well defined operations on $\mathbb{Z}/m\mathbb{Z}$.

Ex. Write down addition and multiplication tables in $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z}$.

By an *inverse* of a modulo m we mean a number c such that $ac \equiv 1 \bmod m$. This is written $c \equiv a^{-1} \mod m$.

An element may or may not have an inverse mod m.

Take $m = 6$. $[5]$ has an inverse in $\mathbb{Z}/6\mathbb{Z}$:

$$[5] \times [5] = [25] = [1]$$

While $[3]$ does not have an inverse : in $\mathbb{Z}/6\mathbb{Z}$ we have $[3][2] = [6] = [0]$. So if $[3]$ had an inverse, say $[a]$, we would have $[3][a] = [1]$, and by miltiplying by $[2]$ we would get $[0] = [2]$ which is not the case.

This suggests that the existence of the inverse of a mod m has something to do with common factors of a and m. This is indeed the case as shown in the following lemma.

Lemma 2.9 *An integer a has an inverse modulo m if and only if a and m are coprime ($\gcd(a, m) = 1$).*

Proof. The integer a has an inverse mod m if and only if the equation

$$ax + my = 1$$

has a solution. This equation has a solution if and only if $\gcd(a, m)$ divides 1 which is only possible if $\gcd(a, m) = 1$. $\square$

As usual, the proof of the lemma gives a procedure for finding inverses. Use Euclidean algorithm to calculate $\gcd(a, m)$. If it's not one, there is inverse. If it is one run the algorithm backwards to find h and k such that $ah + mk = 1$ and

$$[a]^{-1} = [h]$$

Notice in particular that if p is a prime number, then any class $[x] \neq [0]$ is invertible. The set $\mathbb{Z}/p\mathbb{Z}$ is a **field** and it is denoted $\mathbb{F}_p$.

Example 2.10 *Find* $43^{-1} \bmod 7$*.*
Euclid's algorithm :

$$43 = 6 \times 7 + 1$$

They are coprime and $1 = -6 \times 7 + 1 \times 43$*. Hence* $43^{-1} = 1 \bmod 7$
Same with $32^{-1} \bmod 7$*.*

$$\begin{aligned} 32 &= 4 * 7 + 4 \\ 7 &= 1 * 4 + 3 \\ 4 &= 1 * 3 + 1 \end{aligned}$$

And

$$1 = (1*4)+(-1*3) = (-1*7)+(2*4) = (2*32)+(-9*7) = (-9*7)+(2*32)$$

Hence $32^{-1} = 2 \bmod 7$*.*
Same with $49^{-1} \bmod 15$*.*

$$\begin{aligned} 49 &= 3 * 15 + 4 \\ 15 &= 3 * 4 + 3 \\ 4 &= 1 * 3 + 1 \end{aligned}$$

And get

$1 = (1*4)+(-1*3) = (-1*15)+(4*4) = (4*49)+(-13*15) = (-13*15)+(4*49)$

Hence $49^{-1} \mod 15 = 4$.

The equation $ax \equiv b \mod m$**.**

More generally, suppose we want to solve an equation

$$ax = b \mod m$$

By this we mean, find all integers $x \mod m$ that satisfy the equation.

The equation is equivalent to the existence of an integer y such that

$$ax + my = b$$

And we know how to solve this !

This equation has a solution if and only if $d = \gcd(a, b)$ divides b and we know how to find all the solutions.

In particular, the equation has solutions if and only if d divides b.

If this is the case, then to solve the equation, divide it by d, let $a' = a/d,' = m/d, c' = c/d$. Write $a'x + m'y = b'$. Bézout's identity gives (h, k) such that $a'h + m'k = 1$.

By the theorem on solutions of linear diophantine equations, all values of x are $\{b'h + nm'\}$ and the solutions of the equation are the $\{[b'h + nm']\}$. Notice that there are exactly d of them.

Let's see a few examples.

$2x \equiv 4 \mod 10$.

We have $\gcd(2, 10) = 2$, it divides 4, there are solutions. Dividing by 2 we get $x \equiv 2 \mod 5$ i.e $x = 2 + 5n$.

Now the solutions are $\{[2], [7]\}$ (classes $\mod 10$).

The equation $2x = 4 \bmod 5$ has no solutions.

Another example:

$3x \equiv 6 \mod 18$

$\gcd(3, 18) = 3$ divides 6. We find $x \equiv 2 \bmod 6$. Solutions are $\{[2], [8], [14]\}$.

Another: $10x \equiv 14 \mod 18$.

We have $\gcd(10, 14) = 2$, divides 14, we'll find 2 solutions.

Euclid's algorithm gives:

$$\begin{aligned} 18 &= 10 + 8 \\ 10 &= 8 + 2 \\ 8 &= 4 \times 2 + 0 \end{aligned}$$

and Bézout's identity:

$$2 = 10 + (-1) \times 8) = (-1) \times 18 + 2 \times 10)$$

hence

$$14 = -7 \times 18 + 14 \times 10$$

The general solution is $x = 14 + 9n$.

The solutions to the congruence are $\{[14], [5]\}$.

Notice that when a and m are coprime, then there is a unique solution and it is given by $[a]^{-1}[b]$.

For example, solve $99x \equiv 100 \bmod 101$.

99 and 101 are coprime, hence there is a unique solution.

Euclid's algorithm gives:

$$\begin{aligned} 101 &= 99 + 2 \\ 99 &= 2 \times 49 + 1 \\ 2 &= 1 \times 2 + 0 \end{aligned}$$

Bézout's identity:

$$1 = (1 * 99) + (-49 * 2) = (-49 * 101) + (50 * 99)$$

One finds $[99]^{-1} = [50]$. The unique solution is $[50] \times [100] = [5000] = [51]$.

Corollary 2.11 $\mathbb{F}_p^\times = \{[1], [2], \ldots, [p-1]\}$ *is a group with the operation of multiplication.*

Proof. A group is a set with a binary operation (in this case multiplication), such that (i) the operation is associative; (ii) there is an identity element; (iii) every element has an inverse. Clearly [1] is the identity element, and the every element has an inverse because $1, 2, 3 \ldots, p-1$ are coprime with p. $\square$

Recall that Lagrange's theorem states that if G is a finite group and H is a subgroup, then $|H|$ divides $|G|$. The corrolary of this theorem is that if $a \in G$ and $k \geq 0$ is the smallest integer such that $a^k = 1$, then k divides $|G|$.

Theorem 2.12 (Fermat's Little Theorem) *If p is prime and $a \in \mathbb{Z}$ then*

$$a^p \equiv a \mod p.$$

Hence if $p \not| a$ then $a^{p-1} \equiv 1 \mod p$.

Proof. If $p|a$ then $a \equiv 0 \mod p$ and $a^p \equiv 0 \mod p$ so suppose p does not divide a, and so $a \in \mathbb{F}_p^\times$. Recall that by a corollary to Lagrange's Theorem, the order of an element of a group divides the order of the group. Let n be the order of a, so $a^n \equiv 1$. But by the corollary to Lagrange's theorem, $n|p-1$. $\square$

Let's look at an example. What is $33^{22} \mod 23$? 23 is prime so $33^{22} \equiv 1 \mod 23$.

How about $3^{101} \mod 103$? Well 103 is prime so $3^{102} \equiv 1 \mod 103$ So $3^{101} \equiv 3^{-1} \mod 103$. To find $3^{-1} \mod 103$ use Euclid's algorithm.

$$103 = 3 \times 34 + 1.$$

So $3^{-1} \equiv 34 \mod 103$. Hence $3^{101} \equiv 34 \mod 103$.

Another example : 32^6 mod 7. We know that 32^7 mod 32 mod 7. It follows that $32^7 = 32^{-1}$ mod 7. It suffices to calculate 32^{-1} mod 7. We get

$$\begin{aligned} 32 &= 4 * 7 + 4 \\ 7 &= 1 * 4 + 3 \\ 4 &= 1 * 3 + 1 \end{aligned}$$

and

$$1 = (1*4) + (-1*3) = (-1*7) + (2*4) = (2*32) + (-9*7) = (-9*7) + (2*32)$$

Hence $32^{-1} \equiv 2$ mod 7 and $32^6 \equiv 2$ mod 7.

Yet another example : 45^{35} mod 13.

We have $13 \times 2 = 26$ and $45^{13} \equiv 45$ mod 13. Hence, as $35 = 13 \times 2 + 9$, we have $45^{35} = 45^2 \times 45^9 = 45^{11}$ mod 13. As $45^{12} \cong 1$ mod 13, we have $45^{11} = 45^{-1}$ mod 13

We need to calculate 45^{-1} mod 13.

Eucledian algorithm : We get

$$\begin{aligned} 45 &= 3 * 13 + 6 \\ 13 &= 2 * 6 + 1 \end{aligned}$$

and

$$1 = (1 * 13) + (-2 * 6) = (-2 * 45) + (7 * 13) = (7 * 13) + (-2 * 45)$$

Hence $45^{35} \equiv -2 \mod 13 \equiv 11 \mod 13$.

Let's do $43^{42} \mod 13$. We have $43^{39} \equiv 43^3 \mod 13$. Hence $43^{42} \equiv 43^6 \mod 13$.Now $43 \mod 13 \equiv 4 \mod 13$. Hence $43^{42} \equiv 4^6 \mod 13$. Now $4^2 = 16 = 3 \mod 13$ Hence $4^6 = 4^{2^3} = 3^3 = 27 \mod 13 = 1 \mod 13$ Hence $43^{42} \mod 1 \mod 13$.

And now we get to yet another application of the Bézout's lemma.

We would like to find integers z that satisfy **two** congruences: $z \equiv x \mod m$ and $z \equiv y \mod n$.

This is not always possible as the example $z \equiv 3 \mod 4$ and $z \equiv 5 \mod 8$ shows. If such a z existed, one would get $0 = 1 \mod 8$ which is not the case. The reason is that 4 and 8 are not coprime. However, when n and m are coprime, we have the following theorem.

Theorem 2.13 (Chinese Remainder Theorem) *Suppose m and n are coprime; let x and y be two integers. Then there is a unique $[z] \in \mathbb{Z}/nm$ such that $z \equiv x \mod m$ and $z \equiv y \mod n$.*

Proof. (existence) By Bezout's Lemma, we can find $h, k \in \mathbb{Z}$ such that

$$hn + km = 1.$$

Notice that $hn \equiv 1 \mod m$ and $km \equiv 1 \mod n$.

Given x, y we choose z by

$$z = hnx + kmy.$$

Clearly $z \equiv hnx \equiv x \mod m$ and $z \equiv y \mod n$.

(uniqueness) For uniqueness, suppose z' is another solution. Then $z \equiv z' \mod n$ and $z \equiv z' \mod m$. Hence there exist integers r, s such that

$$z - z' = nr = ms.$$

Since $hn + km = 1$ we have

$$z - z' = (z - z')hn + (z - z')km = mshn + nrkm = nm(sh + rk).$$

Hence $z \equiv z'(nm)$. □

As usual the proof gives you a procedure to find z. To find z, find h and k as in the Bézouts lemma (run Euclidean algorithm backwards). Then z is $hnx + kmy$.

Find the unique solution of $x \equiv 3 \mod 7$ and $x \equiv 9 \mod 11$ satisfying $0 \leq x \leq 76$.

Solution find h, k such that $7h + 11k = 1$ using Euclid:
11=7+4
7=4+3
4=3+1
So 1=4-3=4-(7-4)=2.4-7=2.(11-7)-7=2.11-3.7.
Hence let $h = -3$ and $k = 2$ so take $x = -3.7.9 + 2.11.3 = -189 + 66 = -123 \equiv 31 \mod 77$.