MAU23101
Introduction to number theory
1 - Divisibility and factorisation

Nicolas Mascot
mascotn@tcd.ie
Module web page

Michaelmas 2020–2021
Version: October 2, 2020

Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

Main goal of this chapter

Theorem (Fundamental theorem of arithmetic)

Every positive integer can be uniquely decomposed as a product of primes.

Remark

Uniqueness is not obvious!
Given a non-prime integer n, we can write $n = ab$, and continue factoring.
But if we start with $n = a'b'$, will we get the same factors in the end?

Notation

- $\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$.
- $\mathbb{N} = \{1, 2, 3, \cdots\}$.

Remark

In some languages, $\mathbb{N} = \{0, 1, 2, 3, \cdots\}$.

$\rightsquigarrow$ Better notation: $\mathbb{Z}_{\geqslant 1}$.

Smallest and largest elements

Proposition

Let $S \subseteq \mathbb{R}$ be a non-empty, finite subset. Then S has a smallest element, and a largest element.

Counter-example

Not true for $S = \mathbb{R}_{>0} = (0, +\infty)$.

Corollary

Let $S \subseteq \mathbb{N}$, $S \neq \emptyset$. Then S has a smallest element.

Proof.

Since $S \neq \emptyset$, there exists $s_0 \in S$. Let

$$S_{\leqslant s_0} = \{s \in S \mid s \leqslant s_0\}.$$

Then $\min S = \min S_{\leqslant s_0}$, which exists because $S_{\leqslant s_0}$ is finite. □

Application: proof by induction

Theorem (Proof by induction)

Let $P(n)$ be a property depending on $n \in \mathbb{N}$.
If $P(1)$ holds, and if $P(n) \implies P(n+1)$ for all $n \in \mathbb{N}$, then $P(n)$ holds for all $n \in \mathbb{N}$.

Proof.

Suppose not. Then

$$S = \{n \in \mathbb{N} \mid P(n) \text{ does not hold}\}$$

is not empty. Let $n_0 = \min S$. Then $n_0 \neq 1$, so $n_0 - 1 \in \mathbb{N}$.
We have $P(n_0)$ is false, but $P(n_0 - 1)$ is true, because $n_0 - 1 \notin S$ a $n_0 - 1 < \min S$. Absurd. □

Euclidean division in $\mathbb{Z}$

Theorem

Let $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. There exist $q \in \mathbb{Z}$ and $r \in \mathbb{Z}$ such that

$$a = bq + r \quad \text{and} \quad 0 \leqslant r < b.$$

Moreover, q and r are unique.

Euclidean division in $\mathbb{Z}$

Theorem

Let $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. There exist $q \in \mathbb{Z}$ and $r \in \mathbb{Z}$ such that

$$a = bq + r \quad \text{and} \quad 0 \leqslant r < b.$$

Moreover, q and r are unique.

Proof.

Existence: WLOG, assume $a \geqslant 0$. Take

$$q = \max\{x \in \mathbb{Z} \mid bx \leqslant a\} = \max\{x \in \mathbb{Z},\ -a \leqslant x \leqslant a \mid bx \leqslant a\}$$

and $r = a - bq$. Then $bq \leqslant a$, so $r \geqslant 0$. Besides, if $r \geqslant b$, then

$$b(q+1) = bq + b = a \underbrace{-r + b}_{\leqslant 0} \leqslant a,$$

contradiction with the definition of q. □

Euclidean division in $\mathbb{Z}$

Theorem

Let $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. There exist $q \in \mathbb{Z}$ and $r \in \mathbb{Z}$ such that

$$a = bq + r \quad \text{and} \quad 0 \leqslant r < b.$$

Moreover, q and r are unique.

Proof.

Uniqueness: Suppose now $a = bq + r = bq' + r'$ with $0 \leqslant r, r' < b$. Then

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

but also

$$r - r' = (a - bq) - (a - bq') = b(q - q'),$$

whence (divide by b)

$$-1 < \underbrace{q - q'}_{\in \mathbb{Z}} < 1.$$

So $q - q' = 0$, whence $q = q'$ and $r = r'$. □

Divisibility

Divisibility

Definition (Divisibility)

For $a, b \in \mathbb{Z}$, we say that $a \mid b$ if there exists $k \in \mathbb{Z}$ such that $b = ak$.

Remark

$a \mid b$ iff. b is a multiple of a.

Example

- $-2 \mid 6$.
- $1 \mid x$ for all $x \in \mathbb{Z}$.
- $x \mid 1$ iff. $x = \pm 1$.
- If $a \neq 0$, then $a \mid b$ iff. $b/a \in \mathbb{Z}$.
- $0 \mid x$ iff. $x = 0$.
- $x \mid 0$ for all $x \in \mathbb{Z}$.

Divisibility of combinations

Proposition

Let $a, b, c \in \mathbb{Z}$. If $a \mid b$ and $a \mid c$, then

$$a \mid (bx + cy)$$

for all $x, y \in \mathbb{Z}$. In particular,

$$a \mid (b + c) \quad \text{and} \quad a \mid (b - c).$$

Proof.

$a \mid b$ so $b = ak$ for some $k \in \mathbb{Z}$. Similarly $c = al$ for some $l \in \mathbb{Z}$. So

$$bx + cy = akx + aly = a\underbrace{(kx + ly)}_{\in \mathbb{Z}}.$$

□

gcd and lcm

Definition

Let $a, b \in \mathbb{Z}$.

$$\gcd(a, b) = \max\{d \in \mathbb{N} \mid d|a \text{ and } d|b\},$$

$$\operatorname{lcm}(a, b) = \min\{m \in \mathbb{N} \mid a|m \text{ and } b|m\}.$$

Example

For $a = 18$ and $b = 12$, we have

$$\gcd(a, b) = 6, \ \operatorname{lcm}(a, b) = 36.$$

Example

$\gcd(n, n+1) = 1$ for all $n \in \mathbb{Z}$. Indeed, let $d \in \mathbb{N}$ be such that $d \mid n$ and $d \mid (n+1)$; then $d \mid \big((n+1) - n\big) = 1$.

The Euclidean algorithm

Theorem

Let $a, b \in \mathbb{N}$. Start by dividing a by b, then iteratively divide the previous divisor by the previous remainder. The last nonzero remainder is $\gcd(a, b)$.

Example

Take $a = 23$ and $b = 9$. We compute

- $23 = 9 \times 2 + 5$.
- $9 = 5 \times 1 + 4$.
- $5 = 4 \times 1 + 1$.
- $4 = 1 \times 4 + 0$.

$\rightsquigarrow \gcd(23, 9) = 1$.

The Euclidean algorithm

Lemma

Let $a, b \in \mathbb{N}$. *Define*

$$\mathrm{Div}(a,b) = \{d \in \mathbb{N} \mid d|a \text{ and } d|b\},$$

and let $a = bq + r$ *be the Euclidean division. Then*

$$\mathrm{Div}(a,b) = \mathrm{Div}(b,r).$$

Proof.

- $\subseteq$: If $d \mid a$ and $d \mid b$, then $d \mid b$ and $d \mid r = a1 + b(-q)$.
- $\supseteq$: If $d \mid b$ and $d \mid r$, then $d \mid a = bq + r1$ and $d \mid b$.

□

The Euclidean algorithm

Lemma

Let $a, b \in \mathbb{N}$. *Define*

$$\mathrm{Div}(a,b) = \{d \in \mathbb{N} \mid d|a \text{ and } d|b\},$$

and let $a = bq + r$ *be the Euclidean division. Then*

$$\mathrm{Div}(a,b) = \mathrm{Div}(b,r).$$

Proof of the Euclidean algorithm.

Let z be the last nonzero remainder in the Euclidean algorithm. Then

$$\mathrm{Div}(a,b) = \cdots = \mathrm{Div}(\cdots, z) = \mathrm{Div}(z,0) = \mathrm{Div}(z),$$

whence $\gcd(a,b) = \max \mathrm{Div}(a,b) = \max \mathrm{Div}(z) = z$. □

Bézout's theorem

Theorem (Bézout)

Let $a, b \in \mathbb{Z}$. There exist $u, v \in \mathbb{Z}$ such that

$$\gcd(a, b) = au + bv.$$

Bézout's theorem

Theorem (Bézout)

Let $a, b \in \mathbb{Z}$. There exist $u, v \in \mathbb{Z}$ such that

$$\gcd(a, b) = au + bv.$$

Proof.

- $23 = 9 \times 2 + 5$.
- $9 = 5 \times 1 + 4$.
- $5 = 4 \times 1 + 1$.

□

Bézout's theorem

Theorem (Bézout)

Let $a, b \in \mathbb{Z}$. There exist $u, v \in \mathbb{Z}$ such that

$$\gcd(a, b) = au + bv.$$

Proof.

- $5 = 23 - 9 \times 2.$
- $4 = 9 - 5 \times 1.$
- $1 = 5 - 4 \times 1.$

□

Bézout's theorem

Theorem (Bézout)

Let $a, b \in \mathbb{Z}$. There exist $u, v \in \mathbb{Z}$ such that

$$\gcd(a, b) = au + bv.$$

Proof.

- $5 = 23 - 9 \times 2.$
- $4 = 9 - 5 \times 1.$
- $1 = 5 - 4 \times 1.$

$$\begin{aligned} \rightsquigarrow 1 &= 5 - 4 \times 1 \\ &= 5 - (9 - 5 \times 1) \times 1 = 5 \times 2 - 9 \times 1 \\ &= (23 - 9 \times 2) \times 2 - 9 \times 1 = 23 \times 2 - 9 \times 5. \end{aligned}$$

$\square$

Bézout's theorem

Theorem (Bézout)

Let $a, b \in \mathbb{Z}$. There exist $u, v \in \mathbb{Z}$ such that

$$\gcd(a, b) = au + bv.$$

Corollary

Two integers $a, b \in \mathbb{Z}$ are coprime iff. there exist $u, v \in \mathbb{Z}$ such that

$$au + bv = 1.$$

Bézout's theorem

Theorem (Bézout)

Let $a, b \in \mathbb{Z}$. There exist $u, v \in \mathbb{Z}$ such that

$$\gcd(a, b) = au + bv.$$

Corollary

Two integers $a, b \in \mathbb{Z}$ are coprime iff. there exist $u, v \in \mathbb{Z}$ such that

$$au + bv = 1.$$

Example

$\gcd(n, n+1) = 1$ for all $n \in \mathbb{N}$, because
$n \times (-1) + (n+1) \times 1 = 1$.

The fundamental theorem of arithmetic

Prime numbers

Definition (Prime number)

Let $p \in \mathbb{N}$. p is prime if it has exactly two positive divisors. In other words, this means $p \neq 1$ and for all $d \in \mathbb{N}$,

$$d \mid p \iff d = 1 \text{ or } p.$$

An integer $n \geqslant 2$ which is not prime is called composite.

Remark

$n \geqslant 2$ is composite iff. there exist $a, b \in \mathbb{N}$ such that $1 < a, b < n$ and $ab = n$.

Remark

If $p \in \mathbb{N}$ is prime, then for all $n \in \mathbb{Z}$,

$$\gcd(p, n) = \begin{cases} 1, & \text{if } p \nmid n, \\ p, & \text{if } p \mid n. \end{cases}$$

Gauss's lemma

Lemma (Gauss)

Let $a, b, c \in \mathbb{Z}$. *If* $a \mid bc$ *and if* $\gcd(a, b) = 1$, *then* $a \mid c$.

Gauss's lemma

Lemma (Gauss)

Let $a, b, c \in \mathbb{Z}$*. If* $a \mid bc$ *and if* $\gcd(a, b) = 1$*, then* $a \mid c$*.*

Counter-example

$6 \mid 10 \times 3$ but $6 \nmid 10$, $6 \nmid 3$.

Gauss's lemma

Lemma (Gauss)

Let $a, b, c \in \mathbb{Z}$. *If* $a \mid bc$ *and if* $\gcd(a, b) = 1$, *then* $a \mid c$.

Proof.

$\gcd(a, b) = 1$ so $au + bv = 1$ for some $u, v \in \mathbb{Z}$. Then

$$a \mid auc + bcv = (au + bv)c = c.$$

□

Gauss's lemma

Lemma (Gauss)

Let $a, b, c \in \mathbb{Z}$*. If* $a \mid bc$ *and if* $\gcd(a, b) = 1$*, then* $a \mid c$*.*

Corollary (Euclid's lemma)

Let $p \in \mathbb{N}$ *be prime, and let* $b, c \in \mathbb{Z}$*. If* $p \mid bc$*, then* $p \mid b$ *or* $p \mid c$*.*

Gauss's lemma

Lemma (Gauss)

Let $a, b, c \in \mathbb{Z}$. *If* $a \mid bc$ *and if* $\gcd(a, b) = 1$, *then* $a \mid c$.

Counter-example

$6 \mid 10 \times 3$ but $6 \nmid 10$, $6 \nmid 3$.

Corollary (Euclid's lemma)

Let $p \in \mathbb{N}$ *be prime, and let* $b, c \in \mathbb{Z}$. *If* $p \mid bc$, *then* $p \mid b$ *or* $p \mid c$.

Gauss's lemma

Lemma (Gauss)

Let $a, b, c \in \mathbb{Z}$*. If* $a \mid bc$ *and if* $\gcd(a, b) = 1$*, then* $a \mid c$*.*

Corollary (Euclid's lemma)

Let $p \in \mathbb{N}$ *be prime, and let* $b, c \in \mathbb{Z}$*. If* $p \mid bc$*, then* $p \mid b$ *or* $p \mid c$*.*

Proof.

If $p \mid b$, OK. Else, $\gcd(p, b) = 1$; apply Gauss's lemma. □

The fundamental theorem of arithmetic

Theorem

Every $n \in \mathbb{N}$ is a product of primes, and this decomposition is unique (up to re-ordering the factors).

Proof.

Existence: If n is prime, done. Else, $n = ab$ with $1 < a, b < n$; recurse.

Uniqueness: Suppose

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

where the p_i and the q_j are prime. Then

$$p_1 \mid p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s;$$

by applying Euclid's lemma repeatedly, we get $p_1 \mid q_j$ for some j. Since q_j is prime, this forces $p_1 = q_j$. Simplify by $p_1 = q_j$ and start over. $\square$

Practical factoring

Factoring integers

Lemma

Let $n \in \mathbb{Z}_{\geqslant 2}$. If n is composite, there exists prime $p \leqslant \sqrt{n}$ such that $d \mid n$.

Proof.

As n is composite, $n = ab$ with $2 \leqslant a, b < n$. If we had $a, b > \sqrt{n}$, then $n = ab > \sqrt{n}^2 = n$, absurd; So WLOG $a \leqslant \sqrt{n}$. Consider a prime divisor of a. □

Factoring integers

Lemma

Let $n \in \mathbb{Z}_{\geqslant 2}$. If n is composite, there exists prime $p \leqslant \sqrt{n}$ such that $d \mid n$.

Example

Let $n = 23$. Then $\sqrt{n} < \sqrt{25} = 5$, so the primes $\leqslant \sqrt{n}$ are 2 and 3. Since neither divides n, n is prime.

Factoring integers

Lemma

Let $n \in \mathbb{Z}_{\geqslant 2}$. If n is composite, there exists prime $p \leqslant \sqrt{n}$ such that $d \mid n$.

Example

Let $n = 91$. For $p \in \{2, 3, 5\}$, we have $p \mid 90$, so

$$p \mid n \Longrightarrow p \mid (n - 90) = 1;$$

absurd, thus $p \nmid n$.

However $91/7 = 13 \in \mathbb{Z}$, so we have a partial factorisation

$$n = 7 \times 13.$$

If 7 or 13 were composite, they would have a prime factor $p \leqslant \sqrt{13} \leqslant 5$; but then $p \mid 7 \times 13 = n$, absurd. So 7 and 13 are prime, and we have completely factored n.

Valuations

p-adic valuation

Definition

Let $n \in \mathbb{Z}$, $n \neq 0$. Write it as $n = \pm \prod_i p_i^{a_i}$ where $a_i \in \mathbb{Z}_{\geqslant 0}$ and the p_i are distinct primes.
Define $v_{p_i}(n) = a_i$.

Example

$18 = 2^1 \times 3^2$, so $v_2(18) = 1$, $v_3(18) = 2$, $v_p(18) = 0$ for $p \geqslant 5$.

p-adic valuation

Definition

Let $n \in \mathbb{Z}$, $n \neq 0$. Write it as $n = \pm \prod_i p_i^{a_i}$ where $a_i \in \mathbb{Z}_{\geqslant 0}$ and the p_i are distinct primes.
Define $v_{p_i}(n) = a_i$.

Convention: $v_p(0) = +\infty$.

Proposition

Let p be prime. Then for all $m, n \in \mathbb{Z}$,

- $v_p(mn) = v_p(m) + v_p(n)$,
- $v_p(m+n) \geqslant \min\left(v_p(m), v_p(n)\right)$.

Proof.

Exercise! □

Valuations vs. divisibility

Remark

Given integers $m, n, \cdots$, we may always write

$$m = \prod p_i^{a_i}, \quad n = \prod p_i^{b_i}, \cdots$$

with the same distinct primes p_i, by allowing some $a_i, b_i, \cdots$ to be 0.

Lemma

Let $m = \prod_i p_i^{a_i}, n = \prod_i p_i^{b_i} \in \mathbb{N}$, with the p_i distinct primes. Then $m \mid n$ iff. $a_i \leqslant b_i$ for all i.

Example

$$6 = 2^1 3^1 \mid 60 = 2^2 3^1 5^1.$$

$$12 = 2^2 3^1 \nmid 18 = 2^1 3^2.$$

Valuations vs. divisibility

Remark

Given integers $m, n, \cdots$, we may always write
$$m = \prod p_i^{a_i}, \quad n = \prod p_i^{b_i}, \cdots$$
with the same distinct primes p_i, by allowing some $a_i, b_i, \cdots$ to be 0.

Lemma

Let $m = \prod_i p_i^{a_i}, n = \prod_i p_i^{b_i} \in \mathbb{N}$, with the p_i distinct primes. Then $m \mid n$ iff. $a_i \leqslant b_i$ for all i.

Proof.

Exercise! □

Valuations vs. gcd and lcm

Theorem

Let $m = \prod_i p_i^{a_i}, n = \prod_i p_i^{b_i} \in \mathbb{N}$, *with the* p_i *distinct primes.*

$$\textit{Then} \quad \gcd(m, n) = \prod_i p_i^{\min(a_i, b_i)}, \quad \operatorname{lcm}(m, n) = \prod_i p_i^{\max(a_i, b_i)}.$$

Valuations vs. gcd and lcm

Theorem

Let $m = \prod_i p_i^{a_i}, n = \prod_i p_i^{b_i} \in \mathbb{N}$*, with the* p_i *distinct primes.*

Then $$\gcd(m, n) = \prod_i p_i^{\min(a_i, b_i)}, \quad \operatorname{lcm}(m, n) = \prod_i p_i^{\max(a_i, b_i)}.$$

Corollary

The common divisors of m *and* n *are exactly the divisors of* $\gcd(m, n)$*.*

The common multiples of m *and* n *are exactly the multiples of* $\operatorname{lcm}(m, n)$*.*

Valuations vs. gcd and lcm

Theorem

Let $m = \prod_i p_i^{a_i}$, $n = \prod_i p_i^{b_i} \in \mathbb{N}$, *with the* p_i *distinct primes.*

Then $$\gcd(m,n) = \prod_i p_i^{\min(a_i,b_i)}, \quad \operatorname{lcm}(m,n) = \prod_i p_i^{\max(a_i,b_i)}.$$

Corollary

$$\gcd(m,n)\operatorname{lcm}(m,n) = mn \quad \rightsquigarrow \quad \operatorname{lcm}(m,n) = \frac{mn}{\gcd(m,n)}.$$

Proof.

We always have $\min(a,b) + \max(a,b) = a + b$. □

Multiplicative functions

Multiplicative functions

Definition

Let $f : \mathbb{N} \longrightarrow \mathbb{C}$ be a function.

- f *is strongly multiplicative if* $f(mn) = f(m)f(n)$ *for all* $m, n \in \mathbb{N}$.
- f *is (weakly) multiplicative if* $f(mn) = f(m)f(n)$ *for all* $m, n \in \mathbb{N}$ *such that* $\gcd(m, n) = 1$.

We will see examples later!

Sum of geometric progressions

Lemma

Let $x \in \mathbb{C}$, $x \neq 1$; *and let* $n \in \mathbb{N}$. *Then*

$$1 + x + x^2 + x^3 + \cdots + x^n = \frac{x^{n+1} - 1}{x - 1}.$$

Remark

If $x = 1$, what is $1 + x + x^2 + x^3 + \cdots + x^n$?

And what is $\lim_{x \to 1} \frac{x^{n+1} - 1}{x - 1}$?

Sums of powers of divisors

Definition

For $n \in \mathbb{N}$ and $k \in \mathbb{C}$, let $\sigma_k(n) = \sum_{\substack{d \mid n \\ d > 0}} d^k$.

Example

- $\sigma_2(12) = 1^2 + 2^2 + 3^2 + 4^2 + 6^2 + 12^2 = 210$.
- $\sigma_1(n) =$ sum of positive divisors of n.
- $\sigma_0(n) =$ number of positive divisors of n.

Sums of powers of divisors

Definition

For $n \in \mathbb{N}$ *and* $k \in \mathbb{C}$, *let* $\sigma_k(n) = \sum_{\substack{d|n \\ d>0}} d^k$.

Theorem

Let $n = \prod_i p_i^{a_i} \in \mathbb{N}$, *with the* p_i *distinct primes. Then*

$$\sigma_0(n) = \prod_i (a_i + 1), \text{ and}$$

$$\sigma_k(n) = \prod_i \frac{p_i^{k(a_i+1)} - 1}{p_i^k - 1} \text{ for } k \neq 0.$$

Sums of powers of divisors

Proof.

The positive divisors of $n = \prod_{i=1}^{r} p_i^{a_i}$ are the $\prod_{i=1}^{r} p_i^{b_i}$ for all combinations of the b_i such that $0 \leqslant b_i \leqslant a_i$ for all i.
Thus for each i, there are $a_i + 1$ choices for b_i, hence the formula for $\sigma_0(n)$. □

Sums of powers of divisors

Proof.

Similarly, for $k \neq 0$, the k-th power of these divisors are the $\left(\prod_i p_i^{b_i}\right)^k = \prod_{i=1}^r p_i^{kb_i}$, so

$$\begin{aligned}
\sigma_k(n) &= \sum_{\substack{0 \leqslant b_1 \leqslant a_1 \\ \vdots \\ 0 \leqslant b_r \leqslant a_r}} p_1^{kb_1} p_2^{kb_2} \cdots p_r^{kb_r} \\
&= \sum_{b_1=0}^{a_1} \sum_{b_2=0}^{a_2} \cdots \sum_{b_r=0}^{a_r} p_1^{kb_1} p_2^{kb_2} \cdots p_r^{kb_r} \\
&= \left(\sum_{b_1=0}^{a_1} p_1^{kb_1}\right) \left(\sum_{b_2=0}^{a_2} p_2^{kb_2}\right) \cdots \left(\sum_{b_r=0}^{a_r} p_r^{kb_r}\right) \\
&= \prod_{i=1}^{r} \sum_{b_i=0}^{a_i} p_i^{kb_i} = \prod_{i=1}^{r} \frac{p_i^{k(a_i+1)} - 1}{p_i^k - 1}.
\end{aligned}$$

□

The σ_k are multiplicative

Corollary

The σ_k are weakly multiplicative.

Proof.

Let $m, n \in \mathbb{N}$ be coprime. Then $m = \prod p_i^{a_i}$, $n = \prod q_j^{b_j}$ with the p_i distinct from the q_j. □

The Diophantine equation $ax + by = c$

A family of Diophantine equations

Fix integers $a, b, c \in \mathbb{Z}$. We want to solve

$$ax + by = c, \quad x, y \in \mathbb{Z}.$$

A family of Diophantine equations

Fix integers $a, b, c \in \mathbb{Z}$. We want to solve

$$ax + by = c, \quad x, y \in \mathbb{Z}.$$

Example

The equation

$$6x + 10y = 2021$$

has no solutions such that $x, y \in \mathbb{Z}$.

A family of Diophantine equations

Fix integers $a, b, c \in \mathbb{Z}$. We want to solve

$$ax + by = c, \quad x, y \in \mathbb{Z}.$$

Lemma (Strong Bézout)

Let $a, b \in \mathbb{Z}$. The integers of the form $ax + by$ $(x, y \in \mathbb{Z})$ are exactly the multiples of $\gcd(a, b)$.

Proof.

Let $g = \gcd(a, b)$. Then $g \mid a$ and $g \mid b$, so $g \mid (ax + by)$ for all $x, y \in \mathbb{Z}$.
Conversely, by Bézout, we can find $u, v \in \mathbb{Z}$ such that $au + bv = g$; then for all $k \in \mathbb{Z}$,

$$a(ku) + b(kv) = kg.$$

□

A family of Diophantine equations

Lemma (Strong Bézout)

Let $a, b \in \mathbb{Z}$. The integers of the form $ax + by$ $(x, y \in \mathbb{Z})$ are exactly the multiples of $\gcd(a, b)$.

Proof.

Let $g = \gcd(a, b)$. Then $g \mid a$ and $g \mid b$, so $g \mid (ax + by)$ for all $x, y \in \mathbb{Z}$.
Conversely, by Bézout, we can find $u, v \in \mathbb{Z}$ such that $au + bv = g$; then for all $k \in \mathbb{Z}$,

$$a(ku) + b(kv) = kg.$$

□

Corollary

The Diophantine equation $ax + by = c$ has solutions iff. $\gcd(a, b) \mid c$.

Reduction to the case $\gcd(a, b) = 1$

Lemma

Let $a, b \in \mathbb{Z}$ not both zero, and let $g = \gcd(a, b)$. Then the integers $a' = a/g$ and $b' = b/g$ are coprime.

Proof.

By Bézout, we can find $u, v \in \mathbb{Z}$ such that $au + bv = g$. Then $a'u + b'v = 1$, so $\gcd(a', b') = 1$. □

To solve $ax + by = c$ with c a multiple of $g = \gcd(a, b)$, dividing by g yields

$$a'x + b'y = c'$$

where $a' = a/g$, $b' = b/g$, $c' = c/g$

$\rightsquigarrow$ WLOG, we can assume $\gcd(a, b) = 1$.

Solving the case $\gcd(a,b)=1$

Let $a, b, c \in \mathbb{Z}$ be such that $\gcd(a,b)=1$.

Let $x_0, y_0 \in \mathbb{Z}$ such that $ax_0 + by_0 = c$.

Suppose $x, y \in \mathbb{Z}$ also satisfy $ax + by = c$. Then

$$ax_0 + bvy_0 = c = ax + by \ \rightsquigarrow\ a(x_0 - x) = b(y - y_0).$$

So $a \mid b(y-y_0) \underset{\gcd(a,b)=1}{\overset{\text{Gauss}}{\rightsquigarrow}} a \mid (y-y_0)$, whence $y = y_0 + ka$ for some $k \in \mathbb{Z}$.

Similarly, $b \mid a(x_0 - x) \underset{\gcd(a,b)=1}{\overset{\text{Gauss}}{\rightsquigarrow}} b \mid (x_0 - x)$, whence $x = x_0 + lb$ for some $l \in \mathbb{Z}$.

Besides, $a(x_0 - x) = b(y - y_0)$ implies $l = -k$.

Solving the case $\gcd(a, b) = 1$

Proposition

Let $a, b, c \in \mathbb{Z}$ be such that $\gcd(a, b) = 1$. Then $ax + by = c$ has infinitely many solutions. If x_0, y_0 is a solution, then the general solutions are $x = x_0 - kb$, $y = y_0 + ka$ $(k \in \mathbb{Z})$.

Solving the case $\gcd(a, b) = 1$

Proposition

Let $a, b, c \in \mathbb{Z}$ be such that $\gcd(a, b) = 1$. Then $ax + by = c$ has infinitely many solutions. If x_0, y_0 is a solution, then the general solutions are $x = x_0 - kb$, $y = y_0 + ka$ $(k \in \mathbb{Z})$.

Theorem

Let $a, b, c \in \mathbb{Z}$. The Diophantine equation $ax + by = c$ has infinitely many solutions if $\gcd(a, b) \mid c$, and none if $\gcd(a, b) \nmid c$.

Solving the case $\gcd(a, b) = 1$

Example

We want to solve $6x + 10y = 2020$.

$g = \gcd(6, 10) = 2 \mid 2020 \rightsquigarrow$ infinitely many solutions.

Simplify by g: $3x + 5y = 1010$.

Particular solution: Euclidean algorithm gives $3u + 5v = 1$ for $u = 2$, $v = -1 \rightsquigarrow$ can take $x_0 = 2020$, $y_0 = -1010$.
Or directly spot $x_0 = 0$, $y_0 = 202$.

Either way, the solutions are

$$x = x_0 - 5k, \ y = y_0 + 3k, \ k \in \mathbb{Z}.$$

Complements on primes

Infinitely many primes

Theorem (Euclid)

There are infinitely many primes.

Proof.

Suppose not, and let $p_1, \cdots, p_r$ be all the primes. Consider

$$N = p_1 \cdots p_r + 1,$$

and let $p \mid N$ be a prime divisor of N. Then p is one of the p_i, so

$$p \mid p_1 \cdots p_r,$$

thus

$$p \mid (N - p_1 \cdots p_r) = 1,$$

absurd. □

Infinitely many primes

Theorem (Euclid)

There are infinitely many primes.

Example

$p_1 = 3$ is prime.
Prime divisor of $3 + 1 = 4 = 2 \times 2 \rightsquigarrow$ new prime $p_2 = 2$.
Prime divisor of $3 \times 2 + 1 = 7 \rightsquigarrow$ new prime $p_3 = 7$.
Prime divisor of $3 \times 2 \times 7 + 1 = 43 \rightsquigarrow$ new prime $p_4 = 43$.
Prime divisor of $3 \times 2 \times 7 \times 43 + 1 = 13 \times 139 \rightsquigarrow$ new prime $p_5 = 13$ (or 139)...

Infinitely many primes

Theorem (Euclid)

There are infinitely many primes.

Example

$p_1 = 3$ is prime.
Prime divisor of $3 + 1 = 4 = 2 \times 2 \rightsquigarrow$ new prime $p_2 = 2$.
Prime divisor of $3 \times 2 + 1 = 7 \rightsquigarrow$ new prime $p_3 = 7$.
Prime divisor of $3 \times 2 \times 7 + 1 = 43 \rightsquigarrow$ new prime $p_4 = 43$.
Prime divisor of $3 \times 2 \times 7 \times 43 + 1 = 13 \times 139 \rightsquigarrow$ new prime $p_5 = 13$ (or 139)...

Joke

Theorem: There are infinitely many composite numbers.
Proof: Suppose not. Multiply all the composite numbers.
Do not add 1!

The prime number theorem (NON-EXAMINABLE)

Theorem (1896)

For $x \in \mathbb{R}_{\geqslant 0}$, let $\pi(x) = \#\{p \text{ prime} \mid p \leqslant x\}$; for instance $\pi(8.2) = 4$. Then, as $x \to +\infty$,

$$\pi(x) \sim \frac{x}{\log x}.$$

It follows that the n-th prime is $\sim n \log n$ as $n \to +\infty$.

Example

For $x = 10^{10}$, we have

$$\pi(10^{10}) = 455052511 \text{ whereas } \frac{10^{10}}{\log 10^{10}} = 434294481.9032\ldots$$

The billionth prime is

$$p_{10^9} = 22801763489 \text{ whereas } 10^9 \log 10^9 = 20723265836.94\ldots$$

The prime number theorem (NON-EXAMINABLE)

Remark

A better estimate is

$$\pi(x) \sim \mathrm{Li}(x) \stackrel{\text{def}}{=} \int_2^x \frac{dt}{\log t}.$$

The Riemann hypothesis about the complex zeroes of

$$\zeta(s) \stackrel{\text{def}}{=} \sum_{n=1}^{+\infty} \frac{1}{n^s} \stackrel{\text{FTA}}{=} \prod_{p \text{ prime}} \frac{1}{1-p^{-s}}$$

implies

$$\pi(x) - \mathrm{Li}(x) = O(\sqrt{x} \log x).$$

Without it, we can still prove

$$\pi(x) - \mathrm{Li}(x) = O(x/e^{c\sqrt{\log x}}) \text{ for some } c > 0.$$