

Number Theory

Book 2

"Trick" (or technique) for identifying which small integers have the form $x^2 + y^2$ or $x^2 + 3y^2$ or ...

Define $\theta(t) = \sum_{n=-\infty}^{\infty} t^n = 1 + 2t + 2t^4 + 2t^9 + 2t^{16} + 2t^{25} + \dots = \sum_{n \in \mathbb{Z}} t^{n^2}$

$$\theta(t)^2 = (1 + 2t + 2t^4 + 2t^9 + 2t^{16} + 2t^{25} + \dots)(1 + 2t + 2t^4 + 2t^9 + 2t^{16} + 2t^{25} + \dots) = 1 + 4t + 4t^2 + 4t^4 + 8t^5 + 4t^8 + \dots + 12t^{25} + \dots$$

The powers of t appearing in this expansion are precisely the exponents expressible as a sum of two squares. The coefficient of t^n on the right hand side is the number of solutions of $n = x^2 + y^2$ ($x, y \in \mathbb{Z}$)

eg. $25 = x^2 + y^2$ has 12 solutions $(\pm 5, 0), (0, \pm 5), (\pm 3, \pm 4), (\pm 4, \pm 3)$

$5 = x^2 + y^2$ has 8 solutions $(\pm 2, \pm 1), (\pm 1, \pm 2)$

$6 = x^2 + y^2$ has 0 solutions.

$$\theta(t)^3 = 1 + 6t + 12t^2 + 8t^3 + 6t^4 + 24t^5 + 24t^6 + 12t^8 + \dots$$

$1 = x^2 + y^2 + z^2$ has six solutions $(\pm 1, 0, 0), (0, \pm 1, 0), (0, 0, \pm 1)$

$2 = \dots$ twelve $(\pm 1, \pm 1, 0), (\pm 1, 0, \pm 1), (0, \pm 1, \pm 1)$

$7 = x^2 + y^2 + z^2$ has 0 solutions

$\theta(t)^4$ has positive coefficient of t^n for every positive integer n

Lagrange's Theorem: every positive integer is a sum of four squares

Fundamental Theorem of Arithmetic: Every positive integer is uniquely expressible as a product of primes. We'll explain exactly what this says and we'll prove it.

Fundamental Theorem of Calculus
.. .. of Linear Algebra
.. .. of Algebra

FTA = Fundamental Theorem of Arithmetic:

Positive integers factor uniquely as products of primes.

eg. $12 = 6 \times 2 = 2 \times 3 \times 2$

$12 = 3 \times 4 = 3 \times 2 \times 2$

$12 = (-2) \times (-6) = 2 \times 6$

$12 = \boxed{1} \times 12$

Ignore factors of ± 1 in factorization: these are units. (invertible elements). In \mathbb{Z} , the only units are ± 1 .

eg. $\mathbb{Z}[i] = \{a+bi : a, b \in \mathbb{Z}\}$ (commutative ring with identity 1) we again have unique factorization. The units are $\pm 1, \pm i$.

$i \cdot (-i) = 1$

$1 \cdot 1 = 1$

$(-1) \cdot (-1) = 1$

$\mathbb{Z}[i]$ = "Gaussian integers"

$12 = 2 \times 2 \times 3 = \underbrace{(1+i)(1-i)(1+i)(1-i)}_3 = (i-1)(-i-1)(1+i)(1-i) 3$

Cannot be factored any further; they are irreducible.

$2+i = i(1-2i)$

- Elements of \mathbb{R} :
- zero
 - units
 - irreducible
 - reducible.

$10 = 2 \times 5 = (1+i)(1-i)(1+2i)(1-2i) = (1+i)(1-i)(2+i)(2-i)$

$\times i$

$\times (-i)$

"migration of units"

A (commutative ring with identity) has unique factorization if every nonzero element can be factored as a product of irreducible elements and this factorization is essentially unique (ie. unique up to permutation of factors and migration of units).

Why don't we just say primes and composites instead of irreducible and reducible elements?

In \mathbb{Z} :
zero: 0
units: ± 1
irreducible: $\pm 2, \pm 3, \pm 5, \pm 7, \pm 11, \dots$
reducible: $\pm 4, \pm 6, \pm 8, \pm 9, \pm 10, \pm 12, \dots$

In $\mathbb{Z}[i]$:
zero: 0
units: $\pm 1, \pm i$
irreducibles: $\pm 3 = \{1+i, 1-i, -1+i, -1-i\}$
 3 actually 3, -3, 3i, -3i
 $\pm 1 \pm 2i, \pm 2i$
etc.
reducibles: 2 (actually 2, -2, 2i, -2i)

A nonzero element $\alpha \in R$ is reducible if $\alpha \neq 0$, $\alpha \neq \text{unit}$ and $\alpha = \alpha_1 \alpha_2$ with α_1, α_2 not units.

α is irreducible if the only factorizations $\alpha = \alpha_1 \alpha_2$ have either α_1 or α_2 is a unit.

eg. in $\mathbb{Z}[i]$, 3 is irreducible. If $3 = \beta\gamma$, $\beta, \gamma \in \mathbb{Z}[i]$ then either $\beta \in \{\pm 1, \pm i\}$ or $\gamma \in \{\pm 1, \pm i\}$.
2 is reducible since $2 = (1+i)(1-i)$, neither $1+i$ nor $1-i$ is a unit.

Eg. the ring $\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} : a, b \in \mathbb{Z}\}$ does not have unique factorization.

$$\mathbb{Z}[\sqrt{6}] = \{a + b\sqrt{6} : a, b \in \mathbb{Z}\}$$

An example of non-unique factorization in $\mathbb{Z}[\sqrt{6}]$: $6 = 2 \times 3 = \sqrt{6} \times \sqrt{6}$
 $2, 3, \sqrt{6}$ are irreducible in $\mathbb{Z}[\sqrt{6}]$.

But be careful: $\mathbb{Z}[\sqrt{6}]$ has infinitely many units.

Pell's equation $x^2 - 6y^2 = 1$ has solutions $(\pm 1, 0), (\pm 5, \pm 2)$

$x^2 - 6y^2 = -1$ has no integer solutions.

(Look at the equation mod 3)

$$(5 + 2\sqrt{6})(5 - 2\sqrt{6}) = 1 \quad \text{in } \mathbb{Z}[\sqrt{6}]$$

In $\mathbb{Z}[\sqrt{5}]$, the only units are ± 1 .

Unique factorization is not universal.

Difference between $\mathbb{Z}[i], \mathbb{Z}, \mathbb{Z}[\sqrt{2}]$ and $\mathbb{Z}[\sqrt{5}]$
unique factorization

$$15 = 3 \times 5 = (-3) \times (-5) \text{ in } \mathbb{Z}$$

$$15 = 3 \times (2+i) \times (2-i) \text{ in } \mathbb{Z}[i]$$

$$= 3 \times \underbrace{(1+i)}_{\times} \times \underbrace{(1-i)}_{\times} \times 2i$$

$$(2-i)i = 1+2i, (2+i)(i) = 1-2i$$

migration of units

$$15 = 3 \times 5 = (3+3\sqrt{2})(-5+5\sqrt{2}) \text{ in } \mathbb{Z}[\sqrt{2}]$$

$$\underbrace{\quad \quad \quad}_{\times (1+\sqrt{2})} \times \underbrace{\quad \quad \quad}_{\times (-1+\sqrt{2})}$$

Infinitely many units in $\mathbb{Z}[\sqrt{2}]$: solutions of $(a+b\sqrt{2})(a-b\sqrt{2})=1$
 $a^2 - 2b^2 = 1$

$$\pm(1+\sqrt{2})^k = \pm 1, \pm 1\sqrt{2}, \pm 3\pm 2\sqrt{2}, \dots$$

$$3^2 - 2 \cdot 2^2 = (3+2\sqrt{2})(3-2\sqrt{2}) = 1$$

$$6 = 2 \times 3 = (1+\sqrt{5})(1-\sqrt{5})$$

where all factors 2, 3, $1+\sqrt{5}$, $1-\sqrt{5}$ are irreducible in $\mathbb{Z}[\sqrt{5}]$

It holds in $\mathbb{Z}, \mathbb{Z}[i], \mathbb{Z}[\sqrt{2}], \mathbb{Z}[\sqrt{3}], \mathbb{Z}[\sqrt{5}], \mathbb{Z}[\sqrt{2}], \mathbb{Z}[\sqrt{3}]$

Not in $\mathbb{Z}[\sqrt{5}]$ or $\mathbb{Z}[\sqrt{6}]$.

$\mathbb{Z}[\sqrt{5}], \mathbb{Z}[\sqrt{6}]$

non-unique factorization

In $\mathbb{Z}[\sqrt{5}]$ the only units are ± 1 . why
 If x is a unit $x = a+b\sqrt{5}$ then

$$x\bar{x} = (a+b\sqrt{5})(a-b\sqrt{5}) = a^2 - 5b^2 = 1$$

But the only integer solutions are $(a,b) = (\pm 1, 0)$.

$2, 3, 1+\sqrt{5}, 1-\sqrt{5} \in \mathbb{Z}[\sqrt{5}]$ are irreducible.

why? If $2 = \alpha\beta$, $\alpha, \beta \in \mathbb{Z}[\sqrt{5}]$ then

$$\text{then } 4 = |2|^2 = |\alpha|^2 |\beta|^2$$

$$\alpha = a+c\sqrt{5}, \beta = b+d\sqrt{5}$$

$$|\alpha|^2 = (a+c\sqrt{5})(a-c\sqrt{5}) = a^2 - 5c^2$$

$$= a^2 - 5c^2$$

$$|\beta|^2 = b^2 - 5d^2$$

$$4 = |\alpha|^2 |\beta|^2 \text{ where } |\alpha|^2, |\beta|^2 \in \{1, 2, 3, 4, 5, \dots\}$$

$$1 \times 4 \Rightarrow \alpha \text{ unit}$$

$$\frac{2 \times 2}{4 \times 1} \Rightarrow \beta \text{ is a unit.}$$

$a^2 - 5c^2 = 2$ has no solution.

Why does \mathbb{Z} have unique factorization?

It's rather easy to show every integer factors into primes.

$$12 = 3 \times 4 = 3 \times 2 \times 2$$

There is no infinite decreasing sequence $n_1 > n_2 > n_3 > n_4 > \dots > 0$ in the positive integers.

The positive integers are well-ordered. (Equivalently, use induction).

Why is the prime factorization of a positive integer n unique?

Can $n = p_1 p_2 p_3 \dots p_r = q_1 q_2 q_3 \dots q_s$ where $p_1, p_2, \dots, p_r, q_1, q_2, \dots, q_s$ are primes?

We would need to show that every prime on the left (every p_i) occurs also among q_1, \dots, q_s .

Basic step: If p is a prime and $a, b \in \mathbb{Z}$ with $p \mid ab$, then show $p \mid a$ or $p \mid b$.

Euclid's Lemma If a prime p divides ab in \mathbb{Z} , then $p \mid a$ or $p \mid b$.

("or" is inclusive. Eg. $3 \mid 6 \cdot 9 \Rightarrow 3 \mid 6$ or $3 \mid 9$.)

$6 \mid 4 \cdot 9$ but $6 \nmid 4, 6 \nmid 9$. We really need p to be prime.

plh says: $pk = ab$ for some k . Can we argue: p is a prime factor on the left so it's a factor on the right so p is a factor in a or in b . No! This is a common fallacy.

Proof of Euclid's Lemma: Suppose $p|ab$ i.e. $pk=ab$ for some k .
Either $p|a$ or $p|a$. If $p|a$ we're done. Hence we may assume $p \nmid a$.

Then $\gcd(p, a) = 1 = rp + sa$ $\leftarrow p$ not in this list.
for some $r, s \in \mathbb{Z}$.

Divisors of a : $\pm 1, \dots, \pm a$

Divisors of p : $\pm 1, \pm p$.

$b = rbp + sab$ is divisible by p since both terms rbp and sab are divisible by p . \square

If $p|abc$ where p is prime then $p|a$ or $p|b$ or $p|c$.

$p|abc \Rightarrow p|a$ or $p|bc \Rightarrow p|a$ or $p|b$ or $p|c$.

This argument extends to any number of factors i.e. if $p|q_1 q_2 \dots q_l$ where p is prime then $p|q_j$ for some $j \in \{1, 2, \dots, l\}$. (To formalize this argument, use induction.)

Fundamental Theorem of Arithmetic Every positive integer has a unique factorization as a product of primes.

If $n = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$ where $p_1, p_2, \dots, p_r, q_1, q_2, \dots, q_s$ are primes then $p_1|n$ so $p_1|q_j$ for some $j \in \{1, 2, \dots, s\}$ so $p_1 = q_j$. Cancel this prime factor from both sides and repeat the argument with the remaining prime factors.

On to Chapter 9.

Look at powers in $\mathbb{Z}/7\mathbb{Z} = \mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$

$$= \{0, \pm 1, \pm 2, \pm 3\}$$

$$\text{eg. } 3^2 = 9 = 2, \quad \frac{1}{4} = 2.$$

$$-3 = 6+6+6 = 4$$

x	x^0	x^1	x^2	x^3	x^4	x^5	x^6	x^7	x^8
0	1	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1
2	1	2	4	1	2	4	1	2	4
3	1	3	2	6	4	5	1	3	2
$-3 = 4$	1	4	2	1	4	2	1	4	2
$-2 = 5$	1	5	4	6	2	3	1	5	4
$-1 = 6$	1	6	1	6	1	6	1	6	1

palindromic sequence $1, 4, 2, 2, 4, 1$
 $x^5 = x^{-1} = \frac{1}{x}$ if $x \neq 0$

Theorem Let p be prime. Then for all $a \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \dots, p-1\}$, $a^p = a$;

furthermore $a^{p-1} = 1$ if $a \neq 0$.

Remark We really do need p to be prime.

"Fermat's Little Theorem" can be rephrased as:

Let p be prime. Then for all $a \in \mathbb{Z}$, $a^p \equiv a \pmod{p}$. Moreover if $p \nmid a$ (p doesn't divide a) then $a^{p-1} \equiv 1 \pmod{p}$.

Solve the linear system $\begin{cases} 3x + 5y = 2 \\ 4x + 7y = 5 \end{cases}$ for $x, y \in \mathbb{F}_{11} = \{0, 1, 2, \dots, 10\}$

$$\boxed{\frac{1}{3} = 4}$$

$$\begin{bmatrix} 3 & 5 & | & 2 \\ 4 & 7 & | & 5 \end{bmatrix} \sim \begin{bmatrix} 1 & 9 & | & 8 \\ 4 & 7 & | & 5 \end{bmatrix} \sim \begin{bmatrix} 1 & 9 & | & 8 \\ 0 & 4 & | & 6 \end{bmatrix} \sim \begin{bmatrix} 1 & 9 & | & 8 \\ 0 & 1 & | & 7 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & | & 0 \\ 0 & 1 & | & 7 \end{bmatrix}$$

The unique solution is $(x, y) = (0, 7)$.

Check: $(0, 7)$ satisfies both equations.

$$7 - 3 \cdot 6 = 7 - 3 = 4$$

$$5 - 3 \cdot 2 = 5 - 6 = 6$$

$$8 - 6 \cdot 3 + 6 \cdot 6 = 8 - 3 = 0$$

Computing a^p and a^{p-1} may be infeasible but computing $a^p \bmod p$ and $a^{p-1} \bmod p$ is feasible even when a, p are hundreds of digits long.

Mathematica commands `Mod[a^k, n]` computes $a^k \bmod n$. This will fail if a, k are hundreds of digits long. Instead use the command `PowerMod[a, k, n]`

"Modular exponentiation" is a very important operation in cryptography, primality testing, pseudorandom number generation, etc.

Factorization of integers is much harder than primality testing.

(believed to be) non-poly. time.
infeasible

polynomial-time
feasible

Fermat's Little Theorem Let $\mathbb{F}_p = \{0, 1, 2, \dots, p-1\} = \mathbb{Z}/p\mathbb{Z}$ where p is prime. Then $a^p = a$ for all $a \in \mathbb{F}_p$; and $a^{p-1} = 1$ for all nonzero $a \in \mathbb{F}_p$.

Proof Consider the product of all nonzero elements of \mathbb{F}_p : $b = \prod_{0 \neq a \in \mathbb{F}_p} a = 1 \times 2 \times 3 \times \dots \times (p-1) \in \mathbb{F}_p^* = \{1, 2, \dots, p\}$
 (Actually $b = (p-1)!$ but this is now mod p .) Let $a \in \mathbb{F}_p^*$ (nonzero element of \mathbb{F}_p).
 The map $x \mapsto ax$, $\mathbb{F}_p \rightarrow \mathbb{F}_p$ is bijective. (Its inverse is $x \mapsto a^{-1}x$).
 $b = 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1)$
 $a^{p-1}b = a \cdot 2a \cdot 3a \cdot \dots \cdot (p-1)a = b \Rightarrow a^{p-1}bb^{-1} = bb^{-1} \Rightarrow a^{p-1} = 1$.

$\mathbb{F}_p^* = \{1, 2, \dots, p\}$
 = $\{ \text{units in } \mathbb{F}_p \}$
 = $\{ \text{nonzero elements in } \mathbb{F}_p \}$
 Since p is prime

eg. $p=7, a=3, b = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6$
 $3 \cdot 6 \cdot 9 \cdot 12 \cdot 15 \cdot 18$
 $3 \cdot 6 \cdot 2 \cdot 5 \cdot 1 \cdot 4 = b$

For the first conclusion, let $a \in \mathbb{F}_p$ (zero or nonzero).

If $a \neq 0$ then $a \cdot a^{p-1} = 1 \cdot a$ so $a^p = a$. If $a = 0$ then $a^p = 0 = a$. \square

Fermat's Little Theorem is really a special case of Lagrange's theorem in group theory.
 If H is a subgroup of a finite group G then $|H|$ divides $|G|$. In particular the order of every element of G divides $|G|$. So $g^n = 1$ for all $g \in G$ where $n = |G|$.
 \mathbb{F}_p^* is a group of order $p-1$ so $a^{p-1} = 1$ for all $a \in \mathbb{F}_p^*$.

Fermat's Little Theorem plays a huge role in primality testing.

Generalization of Fermat's Little Theorem (Euler's Formula/Theorem) allows us to work with modular exponentiation mod m , m not necessarily prime.

This requires Euler's "totient" function $\phi(m) =$ number of integers $k \in \{1, 2, \dots, m\}$ that are relatively prime to m .
 "Freud"

eg. $\phi(p) = p-1$ whenever p is prime

m	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$\phi(m)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16

1, 2, 3, 4, 5, 6

1, 2, 3, 4, 5

1, 2, 3, 4

$$\phi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p}) \quad (p \text{ prime, } k \geq 1)$$

$$\phi(mn) = \phi(m)\phi(n) \text{ whenever } \gcd(m, n) = 1.$$

$$\phi(5) = 4$$

$$\phi(25) = 20 \neq \phi(5)\phi(5)$$

$$\phi(4) \neq \phi(2)\phi(2)$$

$$\mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$$

$$\text{mod } 2 \begin{array}{|c|} \hline 0 & 1 \\ \hline \end{array}$$

$$\mathbb{Z}/15\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\}$$

$$\phi(15) = 8 = \phi(3)\phi(5)$$

$$\cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$$

$$\phi(30) = \phi(5)\phi(6) = 4 \cdot 2 = 8$$

$$\mathbb{Z}/30\mathbb{Z} = \{0, 1, 2, \dots, 29\}$$

$$\{k \in \mathbb{Z}/30\mathbb{Z} : \gcd(k, 30) = 1\}$$

$$= \{1, 7, 11, 13, 17, 19, 23, 29\}$$

mod 5

	0	1	2	3	4
0	0	6	12	3	9
1	10	1	7	13	4
2	5	11	2	8	14

mod 6

	0	1	2	3	4	5
0	0	25	20	15	10	5
1	6	1	26	21	16	11
2	12	7	2	27	22	17
3	18	13	8	3	28	23
4	24	19	14	9	4	29

mod 5

$(r, s) \in R \oplus S$ is a unit iff r is a unit in R and s is a unit in S .

If R, S are rings then $R \oplus S$ (also denoted $R \times S$) is a ring with componentwise operations
 $(r, s) + (r', s') = (r+r', s+s')$
 $(r, s)(r', s') = (rr', ss')$

For example we look for integer solutions of some Diophantine equation e.g. $61x^2 - y^2 = 91$. Does this have integer solutions? If so, show by example. If not (i.e. no solutions in \mathbb{Z}) then find $m \in \mathbb{Z}$ such that the equation has no solutions in $\mathbb{Z}/m\mathbb{Z}$. In this case it's best to consider prime powers $m = p^k$, p prime, $k \geq 1$.

$x^2 - 3y^2 = 3$ has solutions mod 2 but no solutions mod 4. (So no solutions in \mathbb{Z})
 $x^2 + y^2 + z^2 = 7$ has solutions mod 4 but no solutions mod 8. (-----)

Euler's Formula If a, m are integers, $m \geq 1$ and $\gcd(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$.

This generalizes Fermat's Little Theorem: if p is prime and $\gcd(a, p) = 1$ then $a^{\phi(p)} \equiv 1 \pmod{p}$
 so $a^{p-1} \equiv 1 \pmod{p}$.

The proof of Euler's Formula is the same as the proof of Fermat's Little Theorem.

Both are special cases of Lagrange's Theorem for finite groups.

Eg. Find the last two decimal digits of 1234567^{531}

i.e. find $r \in \{0, 1, 2, \dots, 99\}$ such that $1234567^{531} \equiv r \pmod{100}$.

$$1234567^{531} \equiv 67^{531} \pmod{100}$$

67 is relatively prime to 100 so $67^{\phi(100)} \equiv 1 \pmod{100}$ where $\phi(100) = \phi(2^2 \cdot 5^2) = \phi(2^2) \phi(5^2)$

$$= (2^2 - 2)(5^2 - 5) = 2 \times 20 = 40$$

$$\text{so } 67^{40} \equiv 1 \pmod{100}$$

$$531 = 13 \cdot 40 + 21$$

$$67^{531} = 67^{13 \cdot 40 + 21} = \underbrace{(67^{40})}^1 \cdot 67^{21} \equiv 67^{21} \pmod{100}$$

$$67^{21} \equiv ? \pmod{100}$$

squar $67^1 \equiv 67$

squar $67^2 \equiv 89 \pmod{100}$

squar $67^4 \equiv 89^2 \equiv 21 \pmod{100}$

squar $67^8 \equiv 21^2 \equiv 41 \pmod{100}$

squar $67^{16} \equiv 41^2 \equiv 81 \pmod{100}$

$$67^2 = 4489 \equiv 89 \pmod{100}$$

$$67^{21} = 67^{16} \cdot 67^4 \cdot 67^1 \equiv 81 \cdot 21 \cdot 67 \equiv 67 \pmod{100}$$

so $1234567^{531} \equiv 67 \pmod{100}$

Fast exponentiation using binary representation of the exponent: $21 = 16 + 4 + 1$

i.e. the decimal number 21 is 10101
 16's 8's 4's 2's 1's

Computing $a^k \pmod{m}$ can be done in polynomial time.

decimal 2025 written in binary?

$$\begin{array}{r} 2 \overline{) 2025} \\ \underline{2 \ 1012} \quad r1 \\ 2 \overline{) 506} \quad r0 \\ \underline{2 \ 253} \quad r0 \\ 2 \overline{) 126} \quad r1 \\ \underline{2 \ 63} \quad r0 \\ 2 \overline{) 31} \quad r1 \\ \underline{2 \ 15} \quad r1 \\ 2 \overline{) 7} \quad r1 \\ \underline{2 \ 3} \quad r1 \\ 2 \overline{) 1} \quad r1 \\ \underline{2 \ 0} \quad r1 \end{array}$$

$$2025_{10} = 1111101001_{two}$$

i.e. $2025 = 1024 + 512 + 256 + 128 + 64 + 32 + 16 + 1$

$$x^{2025} = x^{1024} \cdot x^{512} \cdot x^{256} \cdot x^{128} \cdot x^{64} \cdot x^{32} \cdot x^{16} \cdot x^1$$

See Chapter 16: ... repeated squaring.

mod 5

	0	1	2	3	4
0	0	6	12	3	9
1	10	1	7	13	4
2	5	11	2	8	14

Solving a pair of congruences

If $\gcd(m,n)=1$ then the system $\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$

has a unique solution mod mn .

Chapter 11:
Euler's Phi Function
and the Chinese Remainder
Theorem

eg. solve $\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 3 \pmod{5} \end{cases} \iff x \equiv 13 \pmod{15}$.

\iff is trivial. Given $x \equiv 13 \pmod{15}$, we compute

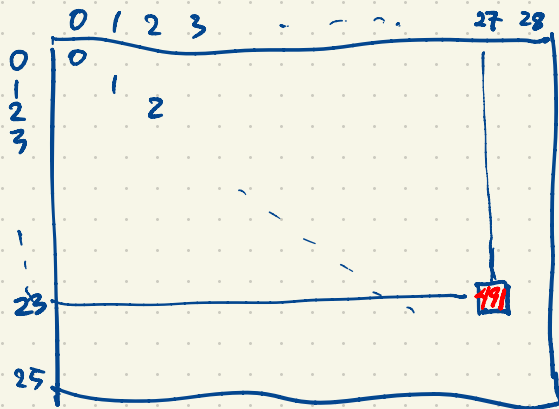
$x \equiv 13 \equiv 1 \pmod{3}$
 $x \equiv 13 \equiv 3 \pmod{5}$

\implies takes a little more work.

eg. $m=26$
 $n=29$ solve $\begin{cases} x \equiv 23 \pmod{26} \\ x \equiv 27 \pmod{29} \end{cases} \iff x \equiv 491 \pmod{754}$

$x \equiv 491 \pmod{754}$
 $26 \cdot 29$

(checked that both the original congruences hold)



Answer without completing all 754 entries in the table.

$$\begin{aligned}
 x &\equiv 23 \pmod{26} \\
 x &= 26k + 23 \equiv 27 \pmod{29} \\
 26k &\equiv 4 \pmod{29} \\
 k &\equiv \underline{-10 \cdot 26} k \equiv -10 \cdot 4 \equiv -40 \equiv -11 \equiv 18 \pmod{29} \\
 &= 1 \pmod{29} \\
 x &= 26(29r + 18) + 23 = 754r + 491 \quad k = 29r + 18
 \end{aligned}$$

Find the inverse of 26 mod 29. ie. $-10 \equiv 19$

29	26	
1	0	29
0	1	26
1	-1	3
-8	9	2
9	-10	1

$\gcd(29,26)=1 = 9 \cdot 29 - 10 \cdot 26$

Ignore this if
you have already done
the survey in another
class



OR

www.uwyo.edu/mathstats

Let us know how you learn in mathematics classes! Please click the button below to access the survey. Thanks!

[View of Learning Mathematics 2025 Survey](#)

$N = \underbrace{1000001!}_{1 \times 2 \times 3 \times \dots \times 1000001} + 1000001$ is divisible by 1000001

$N-1 = 1000001! + 1000000 - \dots - 1000000$

$N-2 = 1000001! + 999999 - \dots - 999999$

$N-3 = 1000001! + 999998 - \dots - 999998$

\vdots
 $N-999999 = 1000001! + 2 - \dots - 2$

None of $N-999999, N-999998, \dots, N$ are prime.

	M	W	F
Mar	24	26	28
	31	2	4
Apr	7	9	11

Test on Ch 1-2 (material before Spring Break) 7:30am Mon Apr 7.
 Expect (i) summary/review sheet and (ii) practice problems this week.

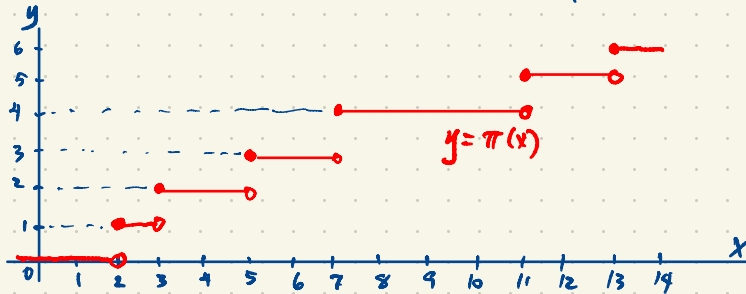
Chapter 13: Counting Primes

$\pi(x)$ = number of primes $\leq x$

eg. $\pi(10) = 4$ since there are exactly four primes ≤ 10 , namely 2, 3, 5, 7

$\pi(10.99999) = 4$

$\pi(11) = 5$ (there are five primes ≤ 11 , namely 2, 3, 5, 7, 11)



The number of primes with at most two decimal digits is $\pi(100) = 25$ (p.92)

The number of primes with exactly three digits is $\pi(1000) - \pi(100) = 168 - 25 = 143$.

The number of primes in $(a, b]$ is $\pi(b) - \pi(a)$
 no. of primes in $[0, b]$ no. of primes in $[0, a]$

How fast does $\pi(x)$ grow as $x \rightarrow \infty$? Slower than linear:

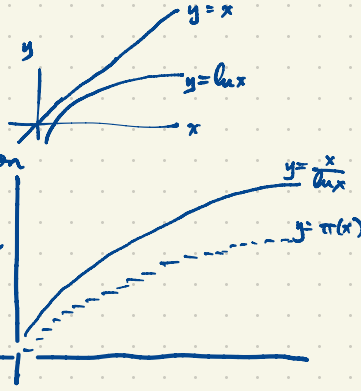
$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x} = 0$$

$$\zeta(x) = \sum_{n=1}^{\infty} \frac{1}{n^x}$$

Prime Number Theorem

$$\pi(x) \sim \frac{x}{\ln x}$$

Proof uses $\zeta(x)$ = Riemann zeta function
Independently proved by Hadamard
and de la Vallée Poussin 1896



i.e. $\lim_{x \rightarrow \infty} \frac{\pi(x)}{x/\ln x} = 1$ i.e. $\frac{\pi(x)}{x/\ln x} \rightarrow 1$ as $x \rightarrow \infty$.

Selberg and Erdős gave more elementary proofs 1949

$\pi(10^{29})$ = how many primes have at most 29 decimal digits

$$= 1\ 520\ 698\ 109\ 714\ 272\ 166\ 094\ 258\ 063$$

$$\frac{10^{29}}{\ln 10^{29}} = 1\ 573\ 829\ 040\ 451\ 813\ 892\ 012\ 209\ 509 \dots$$

$$Li(10^{29}) = 1\ 520\ 698\ 109\ 714\ 276\ 717\ 287\ 880\ 527 \dots$$

Alternative form of PNT (Prime Number Theorem):

For N large, the number of primes in $(N, N+\Delta N]$ is ΔN smaller than N is

$$\pi(N+\Delta N) - \pi(N) \approx \frac{\Delta N}{\ln N}$$

i.e. for numbers $n \approx N$ chosen randomly, the probability that n is prime is about $\frac{1}{\ln N}$.

For random 100-digit numbers, the probability of being prime is $\frac{1}{\ln 10^{100}} \approx 0.00434$ i.e. 0.4%

old numbers, this leads to a better estimate for $\pi(x) \approx Li(x) = \int_2^x \frac{dt}{\ln t}$ $\frac{2}{\ln 10^{100}} \approx 0.0087$ almost 1%.

$$\pi(x) \sim Li(x) \sim \frac{x}{\ln x}$$

$$\sqrt{x^2 + 2x} \sim x \text{ as } x \rightarrow \infty$$

Since $\frac{\sqrt{x^2 + 2x}}{x} = \sqrt{1 + \frac{2}{x}} \rightarrow 1$ as $x \rightarrow \infty$.

but $\sqrt{x^2 + 2x} - x \rightarrow 1$ as $x \rightarrow \infty$.

$$\sqrt{x^6 + x^5} \sim x^3 \text{ as } x \rightarrow \infty$$

$$\frac{\sqrt{x^6 + x^5}}{x^3} \rightarrow 1 \text{ as } x \rightarrow \infty$$

But $\sqrt{x^6 + x^5} - x^3 \rightarrow \infty$ as $x \rightarrow \infty$.

googol = 10^{100}

The Euler totient function $\phi(n)$ = the number of integers k , $1 \leq k \leq n$, satisfying $\gcd(k, n) = 1$.

This function is multiplicative: $\phi(mn) = \phi(m)\phi(n)$ whenever $\gcd(m, n) = 1$.

eg. $\phi(15) = \phi(3)\phi(5)$ since $\gcd(3, 5) = 1$.

$$\frac{\phi(15)}{8} = 2 \times 4$$

1, 2, 4, 7, 8, 11, 13, 14 relatively prime with 15

1, 2 rel. prime to 3

1, 2, 3, 4 rel. prime to 5

$\phi(p) = p - 1$
whenever p is prime

$$\phi(32) \neq \phi(4)\phi(8)$$

$$16 \neq 2 \cdot 4$$

1, 3 rel. prime to 4

1, 3, 5, 7 rel. prime to 8

1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31 rel. prime to 32

If $f(mn) = f(m)f(n)$ for all m, n integers, we say f is completely multiplicative.

Next: some more examples of multiplicative functions.

$\sigma(m)$ = sum of the positive integer divisors of m

eg. $\sigma(12) = 1+2+3+4+6+12 = 28 =$

$$\sigma(10) = 1+2+5+10 = 18 = (1+2)(1+5) = \sigma(2)\sigma(5)$$

$$\sigma(11) = 1+11 = 12$$

$$\sigma(p) = p+1 \iff p \text{ is prime}$$

$$12 = 4 \cdot 3$$

$$\sigma(12) = (1+2+4)(1+3) = \sigma(4)\sigma(3)$$

σ is a multiplicative function: $\sigma(mn) = \sigma(m)\sigma(n)$ whenever $\gcd(m,n)=1$.

$$12 = 2 \cdot 6 \quad \text{but } 28 = \sigma(12) \neq \sigma(2)\sigma(6) = (1+2)(1+2+3+6) = 3 \cdot 12 = 36$$

of course the sum of all divisors of 6 is $(-6)+(-3)+(-2)+(-1)+1+2+3+6=0$

The perfect number problem: When can the sum of the proper positive divisors of n be equal to n ? Historically such numbers were called perfect. eg. $6 = 1+2+3$ is perfect. n is perfect iff $\sigma(n) = 2n$.

$$\sigma(6) = \underbrace{1+2+3}_{6} + 6 = 2 \cdot 6 = 12.$$

28 is also perfect: $28 = 1 + 2 + 4 + 7 + 14$

$$\sigma(28) = \underbrace{1 + 2 + 4 + 7 + 14}_{28} + 28 = 2 \cdot 28 = 56.$$

$$28 = 4 \cdot 7$$

$$\sigma(28) = \sigma(4)\sigma(7) = (1+2+4)(1+7) = 7 \cdot 8 = 56.$$

The smallest perfect numbers are $6, 28, 496 = 16 \cdot 31$

$$\sigma(496) = \sigma(16)\sigma(31) = (1+2+4+8+16)(1+31) = 31 \cdot 32 = 2 \cdot 496$$

$$\begin{array}{r} 31 \\ 16 \\ \hline 186 \\ 31 \\ \hline 496 \end{array}$$

Open questions:

- Are there any odd perfect numbers?
- Are there infinitely many perfect numbers?

$\sigma(p) = p+1$ whenever p is prime

$$\sigma(p^k) = 1 + p + p^2 + \dots + p^k = \frac{p^{k+1} - 1}{p - 1} \quad \text{since } (p-1)(1 + p + p^2 + \dots + p^k) = -1 + p - p + p^2 - p^2 + \dots + p^k - p^k + p^k = p^{k+1} - 1$$

$$\sigma(16) = \sigma(2^4) = \frac{2^5 - 1}{2 - 1} = 31$$

One way (maybe the only way?) to get a perfect number is to find a prime number p such that $2^p - 1$ is prime and then take $n = 2^p(2^p - 1)$

$$\sigma(n) = \sigma(2^p) \sigma(2^p - 1) = \frac{2^{p+1} - 1}{2 - 1} (2^p - 1 + 1) = (2^p - 1) 2^p = 2n$$

How often is $2^p - 1$ a prime number?

Denote $M_p = 2^p - 1$.

p	M_p	
1	$2^1 - 1 = 1$	not prime
2	$2^2 - 1 = 3$	is prime
3	$2^3 - 1 = 7$	is prime
4	$2^4 - 1 = 15$	is not prime
5	$2^5 - 1 = 31$	is prime
6	$2^6 - 1 = 63$	is not prime
7	$2^7 - 1 = 127$	is prime
8	$2^8 - 1 = 255$	is not prime
9	$2^9 - 1 = 511$	is not prime
10	$2^{10} - 1 = 1023$	is not prime
11	$2^{11} - 1 = 2047 = 23 \times 89$	is not prime.

$2^{ab} - 1$ is divisible by $2^a - 1$

$$x^k - 1 = (x - 1)(1 + x + x^2 + \dots + x^{k-1})$$

Let $x = 2^a$, $k = b$.

$$2^{ab} - 1 = (2^a - 1)(1 + 2^a + 2^{2a} + \dots + 2^{(b-1)a})$$

giving a nontrivial factorization of $2^{ab} - 1$ if $a, b > 1$.

In order for a number of the form

$M_p = 2^p - 1$ to be prime, we require p to be prime.

However the converse fails: if p is prime, it does not follow that $M_p = 2^p - 1$ is prime.

Primes of the form $M_p = 2^p - 1$ (p prime)
are called Mersenne primes.

Only 52 Mersenne primes are known : see GIMPS

Theorem Let n be an even integer. Then n is perfect iff $n = 2^{p-1}(2^p - 1)$
where p and $2^p - 1$ are prime. Thus we have a one-to-one correspondence
between even perfect numbers and Mersenne primes

$$n = 2^{p-1}(2^p - 1) \iff M_p = 2^p - 1$$

In particular exactly 52 perfect numbers are known.

We don't know whether there are infinitely many Mersenne primes and
we don't know whether there are any odd perfect numbers.

Proof of the theorem. In one direction we have seen that if p and

$M_p = 2^p - 1$ are prime then $\sigma(n) = 2n$.

Conversely, suppose n is an even perfect number; we must show that
 $n = 2^{p-1}(2^p - 1)$ where p and $2^p - 1$ are prime. Now $n = 2^k m$ where $k \geq 1$
and m is odd. Since n is perfect, $2^k m = 2n = \sigma(n) = \sigma(2^k) \sigma(m) = \frac{2^{k+1} - 1}{2 - 1} \sigma(m)$
where $2^{k+1} - 1$ is odd, so $2^{k+1} \mid \sigma(m)$. (Euclid's Lemma) $= (2^{k+1} - 1) \sigma(m)$

Now $\sigma(m) = 2^{k+1}c$ for some positive integer c and

$$2^{k+1}m = (2^{k+1}-1)\sigma(m) = (2^{k+1}-1)2^{k+1}c \Rightarrow m = (2^{k+1}-1)c.$$

If $c > 1$ then $2^{k+1}c = \sigma(m) \geq \underbrace{1+c+m}_{\text{distinct divisors of } m} = 1+c+(2^{k+1}-1)c = 1+2^{k+1}c$, a contradiction.

so $c=1$, $m=2^{k+1}-1$,
 $\sigma(m) = 1+m$, m is prime hence a Mersenne prime so $k+1=p$ is prime
and $n = 2^k m = 2^{p-1}(2^p-1)$. \square

The largest known primes are Mersenne primes. (Here we're looking just at the explicitly known primes.) This is likely to be the case in the future as more primes are discovered. Mersenne numbers $M_n = 2^n - 1$ are easier to check for primality than other numbers. The lamplighter effect.

What are large primes good for? (The largest Mersenne primes, i.e. the largest known primes, are currently tens of millions of decimal digits long.) The largest primes used in cryptographic applications currently, are only a few hundred digits long, possibly a few thousand digits if you're paranoid.

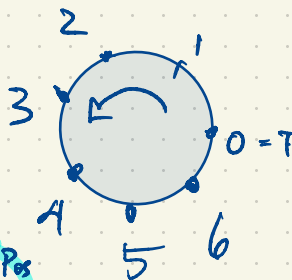
$\mathbb{F}_p = \{0, 1, 2, \dots, p-1\}$ where p is prime

Eg. $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$

\mathbb{R} is an ordered field; \mathbb{F}_7 is not an ordered field.

\mathbb{C} is not an ordered field.

Is $i > 0$ or $i < 0$?
 Pos \times Pos = Pos Neg \times Neg = Pos
 ~~$i \times i = -1 > 0$ $i \times i = -1$~~



Instead of "positive" and "negative" in \mathbb{F}_7 , we talk about ^(nonzero) squares and nonsquares
 1, 2, 4 3, 5, 6

a	a^2	a	a^2
0	0	0	0
1	1	± 1	1
2	4	± 2	4
3	2	± 3	2
$-3=4$	2		
$-2=5$	4		
$-1=6$	1		

Multiplication Table

	0	1	2	4	3	5	6
0	0	0	0	0	0	0	0
1	0	1	2	4	3	5	6
2	0	2	4	1	6	3	5
4	0	4	1	2	5	6	3
3	0	3	6	5	2	1	4
5	0	5	3	6	1	4	2
6	0	6	5	3	4	2	1

Ignoring zero,

- (i) Square \times Square = Square
- (ii) Nonsq \times Nonsq = Square
- (iii) Sq \times Nonsq = Nonsq
- (iv) Nonsq \times Sq = Nonsq

These rules hold in \mathbb{F}_p whenever p is an odd prime. Why?

In \mathbb{R} , pos + pos = pos
 pos \times pos = pos

In \mathbb{F}_7 ,
~~sq \times sq = sq~~
~~sq + sq = sq~~
 $1 + 2 = 3$
~~sq sq nonsq~~

(i) is obvious since $a^2 \times b^2 = (ab)^2$

(iii) follows by process of elimination; similarly (iv).

(ii)

If p is an odd prime then \mathbb{F}_p has $p-1$ nonzero elements, $1, 2, \dots, p-1$, half of which are squares and the other half are nonsquares.

There are $\frac{p-1}{2}$ (nonzero) squares and $\frac{p-1}{2}$ nonsquares.

Eg. $p=11$

a	a^2
0	0
± 1	1
± 2	4
± 3	9
± 4	5
± 5	3

$p=5$

a	a^2
0	0
± 1	1
± 2	4

(Nonzero) squares: 1, 4
nonsquares: 2, 3

$p=3$:

a	a^2
0	0
± 1	1

(Nonzero) squares: 1
nonsquares: 2

(nonzero) squares: 1, 3, 4, 5, 9
Nonsquares: 2, 6, 7, 8, 10

Use Fermat's Little Theorem: Let p be an odd prime. For all $a \in \mathbb{F}_p$, $a^p = a$
In other words, the polynomial $f(x) = x^p - x$ has every element of \mathbb{F}_p as a root. $a^{p-1} = 1 \quad \forall a \neq 0$

for $p=7$, $f(x) = x^7 - x$ has 7 distinct roots in \mathbb{F}_7 .

$$= \underbrace{x}_{x=0} (x-1) (x-2) (x-3) (x-4) (x-5) (x-6)$$

$$f(x) = x(x^6 - 1) = x(x^3 + 1)(x^3 - 1)$$

roots: 0 roots: 3, 5, 6 (nonsquares) roots: 1, 2, 4 (squares)