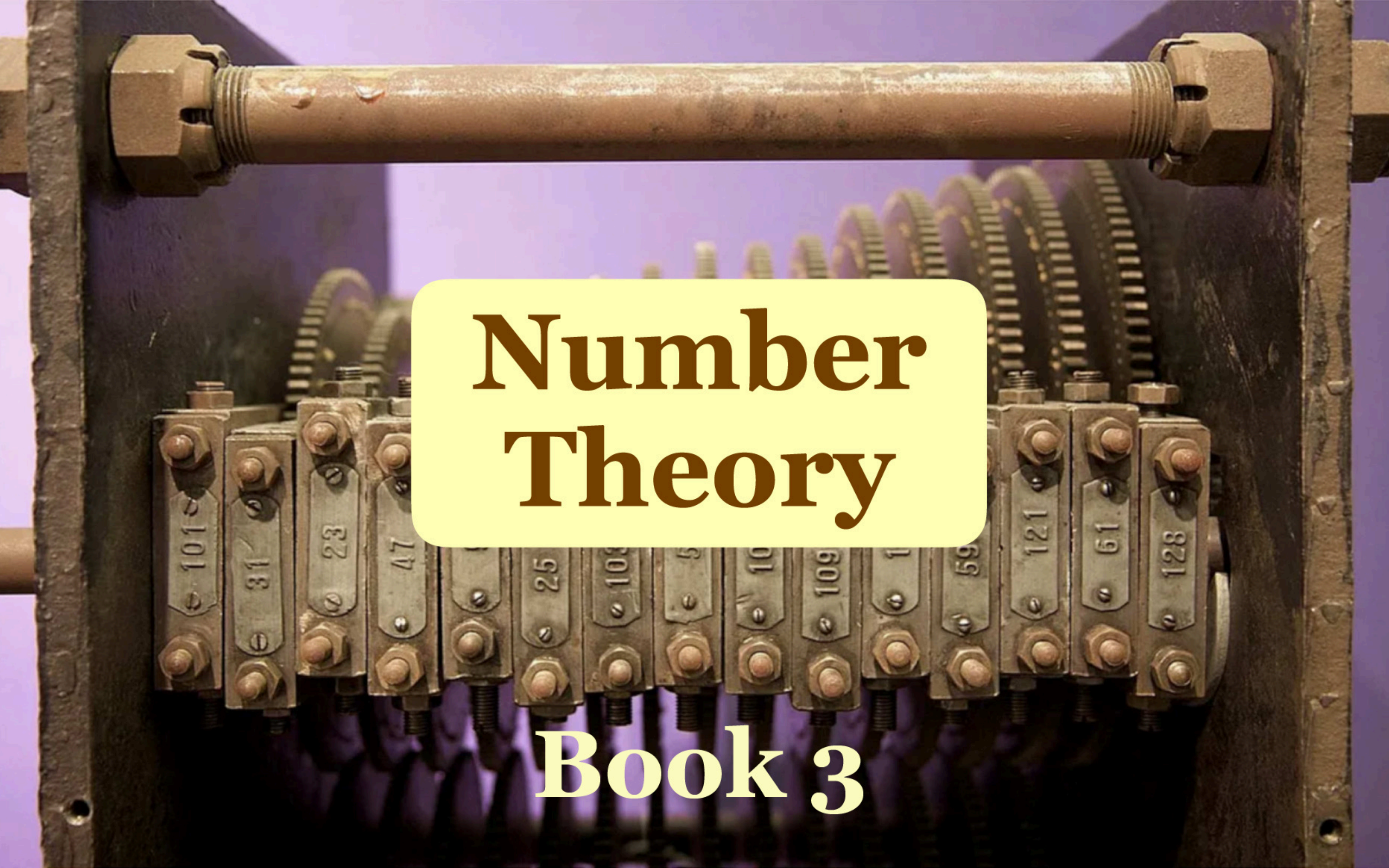
Number Theory

Book 3



Theorem Let p be an odd prime. Then

$$x^p - x = x(x^{p-1}-1) = x\left(x^{\frac{p-1}{2}}-1\right)\left(x^{\frac{p-1}{2}}+1\right) = x(x-1)(x-2)\cdots(x-(p-1))$$

- $x^{\frac{p-1}{2}}-1$ — Roots: all (nonzero) squares in $\mathbb{F}_p$
- $x^{\frac{p-1}{2}}+1$ — Roots: all nonsquares in $\mathbb{F}_p$.
- $x(x-1)(x-2)\cdots(x-(p-1))$ — Every $a \in \mathbb{F}_p$ is a root of $x^p - x$. (Fermat's Little Theorem)

Proof Let $a \in \mathbb{F}_p$, $a \neq 0$, so a^2 is a nonzero square in $\mathbb{F}_p$. Then a^2 is a root of $x^{\frac{p-1}{2}}-1$ since $(a^2)^{\frac{p-1}{2}}-1 = a^{p-1}-1 = 0$ by Fermat's Little Theorem.
So by process of elimination, $x^{\frac{p-1}{2}}+1$ has as its $\frac{p-1}{2}$ roots all the nonsquares in $\mathbb{F}_p$

This gives a criterion for checking when an element $a \in \mathbb{F}_p$ is a square or a nonsquare. called **Euler's Criterion**: given $a \in \mathbb{F}_p$, p an odd prime,

$$a^{\frac{p-1}{2}} \equiv \begin{cases} 1 & \text{if } a \text{ is square nonzero} \\ -1 & \text{if } a \text{ is nonsquare} \\ 0 & \text{if } a = 0. \end{cases} \mod p.$$

Eg. is 7 a square or a nonsquare in $\mathbb{F}_{13}$? Use Euler's Criterion: $7^6 \equiv 10^3 \equiv 1000 \equiv 12 \equiv -1 \mod 13$
So 7 is a nonsquare mod 13.

Definition Let p be an odd prime, $a \in \mathbb{Z}$. Then the Legendre symbol $\left(\frac{a}{p}\right) \in \{-1, 0, 1\}$ is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is nonzero square mod } p; \\ -1 & \text{if } a \text{ is nonsquare mod } p; \\ 0 & \text{if } a \equiv 0 \mod p. \end{cases}$$

So $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \mod 13$.

eg. $\left(\frac{7}{13}\right) = -1$, $\left(\frac{10}{13}\right) = 1$, $\left(\frac{0}{13}\right) = 0$, $\left(\frac{39}{3}\right) = 0$, $\left(\frac{20}{13}\right) = -1$

$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ for all $a, b \in \mathbb{Z}$ (they don't need to be relatively prime)

The Legendre symbol $\left(\frac{a}{p}\right)$ is a completely multiplicative function of a (where the odd prime p is fixed)

eg. $\underbrace{\left(\frac{20}{13}\right)}_{-1} = \underbrace{\left(\frac{4}{13}\right)}_{+1}\underbrace{\left(\frac{5}{13}\right)}_{-1} = -1$ so $20 \equiv 7 \bmod 13$ is a nonsquare mod 13.

When is $\underset{\equiv p-1}{-1}$ a square mod p? -1 is a $\begin{cases} \text{nonsquare mod } 3, 7, 11, \ldots, 2003, \ldots \\ \text{square mod } 5, 13 \end{cases}$

Is -1 a square or a nonsquare mod $p = 2003$? Nonsquare.

<u>Theorem</u> Let p be an odd prime. Then $\left(\frac{p-1}{p}\right) = \left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \bmod 4 \\ -1 & \text{if } p \equiv 3 \bmod 4. \end{cases}$

The quick proof uses $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \bmod p$

If $p = 4k+1$ then $\frac{p-1}{2} = 2k$, $(-1)^{2k} = 1$.

If $p = 4k+3$ then $\frac{p-1}{2} = 2k+1$, $(-1)^{2k+1} = -1$.

How hard is it to find a nonsquare mod p (given an odd prime p)?

Given $a \in \mathbb{Z}$, p odd prime, compute the Legendre symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ nonzero square mod } p \\ 0 & \text{if } a \equiv 0 \bmod p \\ -1 & \text{if } a \text{ nonsquare mod } p \end{cases}$$

We can use Euler's Criterion $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$. Easy on a computer; not so easy by hand. But there is a method that works well by hand: the method of Quadratic Reciprocity (Ch. 22).

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

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p \equiv 1 \bmod 4 \\ -1 & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \bmod 8 \\ -1 & \text{if } p \equiv \pm 3 \bmod 8 \end{cases}$$

eg. $\left(\frac{2}{7}\right) = 1$ since $2 \equiv 3^2 \bmod 7$

$7 \equiv -1 \bmod 8$ so ...

$\left(\frac{2}{5}\right) = -1$ 1,4 squares mod 5
2,3 nonsquares ...

If $p \neq q$ odd primes then $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ are closely related:

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \quad \text{if at least one of } p, q \text{ is } \equiv 1 \bmod 4$$

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right) \quad \text{if } p \equiv q \equiv 3 \bmod 4$$

i.e. $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$ (the law of Quadratic Reciprocity)

Eg. Compute $\left(\frac{14}{47}\right) = \underbrace{\left(\frac{2}{47}\right)}_{+1}\left(\frac{7}{47}\right) = \left(\frac{7}{47}\right) = -\left(\frac{47}{7}\right) = -\left(\frac{5}{7}\right) = -(-1) = 1$ i.e. 14 is a square mod 47.

since $47 \equiv -1 \bmod 8$; since $7 \equiv 47 \equiv 3 \bmod 4$

Eg. $\left(\frac{60}{89}\right) = \left(\frac{2^2\cdot 3\cdot 5}{89}\right) = \underbrace{\left(\frac{2}{89}\right)^2}_{+1}\left(\frac{3}{89}\right)\left(\frac{5}{89}\right) = \left(\frac{3}{89}\right)\left(\frac{5}{89}\right) = \left(\frac{89}{3}\right)\left(\frac{89}{5}\right) = (-1)\left(\frac{4}{5}\right) = (-1)(+1) = -1$

$89 \equiv 1 \bmod 4$; i.e. 60 is a nonsquare mod 89.

Questions: If we compute $\left(\frac{a}{p}\right) = 1$ (either by Euler's Criterion or Quadratic Reciprocity) we know $x^2 \equiv a \bmod p$ has two solutions (the two square roots of a mod p). Can we actually find these two solutions? (i.e. compute the square roots of a mod p)? Yes.

eg. $p \equiv 1 \bmod 4$, $\left(\frac{-1}{p}\right) = +1$. In this case we can find the two square roots of -1 mod p rather easily even if p is thousands of digits long. As follows:

Pick $c \in \{1, 2, \cdots, p-1\}$ randomly. Compute $\left(\frac{c}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \bmod p$.

If $\left(\frac{c}{p}\right) = -1$ (c is nonsquare mod p) take $x \equiv c^{\frac{p-1}{4}} \bmod p$, then $x^2 \equiv c^{\frac{p-1}{2}} \equiv -1 \bmod p$

If $\left(\frac{c}{p}\right) = +1$ (c square mod p) try again.

99.9% of the time, it takes at most ten tries to find x satisfying $x^2 \equiv -1 \bmod p$.

How can we find $a, b \in \mathbb{Z}$ satisfying $p = a^2 + b^2$? (assuming $p \equiv 1 \bmod 4$)

This is as difficult of finding a solution of $x^2 \equiv -1 \bmod p$.

If $p = a^2 + b^2$ then in $\mathbb{F}_p$, $a^2 + b^2 = 0$, $b^2 = -a^2$, $-1 = \left(\frac{a}{b}\right)^2$. The square roots of -1 mod p are $\pm\frac{a}{b}$.

Theorem Let p be prime. Then p is a sum of two squares iff $p \not\equiv 3 \bmod 4$.

Proof We already know that if $p \equiv 3 \bmod 4$ then p is not a sum of two squares. Conversely, suppose p is prime, $p \not\equiv 3 \bmod 4$. There is more than one proof but we will give an algorithm solution which tells us how to find $a, b \in \mathbb{Z}$ such that $a^2+b^2=p$. This algorithm is very efficient in practice even for primes having hundreds or thousands of decimal digits. If $p=2$ then $p=1^2+1^2$. Henceforth $p \equiv 1 \bmod 4$. Let $c \in \{1, \dots, p-1\}$ such that $c^2 \equiv -1 \bmod p$. (See previous slide for a method to find c.) Then $c^2+1 \equiv 0 \bmod p$ i.e. $c^2+1 = mp$ for some $m \geq 1$. We can iterate the ~~following~~ descent step which leads from a large multiple of p as $\square^2+\square^2$, to a smaller multiple of p of this form, repeating until we get $p = a^2+b^2$, $a, b \in \mathbb{Z}$.

(Fermat's Method of Descent)

Suppose $mp = a^2+b^2$, $a, b \in \{\pm 1, \pm 2, \cdots, \pm \frac{p-1}{2}\}$. So $mp = \alpha\bar{\alpha}$, $\alpha = a+bi \in \mathbb{Z}[i]$

After reducing $a, b \bmod m$ to get $\alpha \equiv \beta \bmod m$ where $\beta = a'+b'i$, $|a'|, |b'| \leq \frac{m}{2}$ (choose $a', b' \in \{-\frac{m}{2}, \dots, \frac{m}{2}\}$ or $\{\frac{-m+1}{2}, \dots, \frac{m-1}{2}\}$)

$a \equiv a' \bmod m$
$b \equiv b' \bmod m$

Then $\alpha\bar{\beta} = m\gamma$ for some $\gamma \in \mathbb{Z}[i]$.

since $\alpha\bar{\beta} = (a+bi)(a'-b'i) = \underbrace{(aa'+bb')}_{\equiv a^2+b^2 = mp \equiv 0 \bmod m} + \underbrace{(a'b-ab')}_{\equiv ab-ab \equiv 0 \bmod m} i$

$\alpha\bar{\alpha} = mp$

$\alpha\bar{\alpha}\beta\bar{\beta} = mp\beta\bar{\beta}$

$(\alpha\bar{\beta})(\bar{\alpha}\beta) = mp\beta\bar{\beta}$

$m\gamma \cdot m\bar{\gamma} = mp\beta\bar{\beta}$

$m\gamma\bar{\gamma} = p\beta\bar{\beta}$ where p divides both sides so $\gamma\bar{\gamma} = pk$

$mpk = p\beta\bar{\beta}$

$mk = \beta\bar{\beta}$

$m^2\gamma\bar{\gamma} = mp\beta\bar{\beta} = mp \cdot mk$

$\gamma\bar{\gamma} = pk$. where we can check $1 \leq k < m$.

This can be checked carefully to finish the proof.

Eg. Write $p=1009$ as a sum of two squares. ($1009 \equiv 1$ prime)

$2^{\frac{p-1}{2}} \equiv 1 \mod p$ so $\left(\frac{2}{p}\right) = 1$

$13^{\frac{p-1}{2}} \equiv -1 \mod p$ so 13, 31 nonsquares mod $p = 1009$.

$31^{\frac{p-1}{2}} \equiv -1 \mod p$

$13^{\frac{p-1}{4}} \equiv 469 \mod p$

$31^{\frac{p-1}{4}} \equiv 540 \mod p$

The two square roots of -1 mod p are ± 469 ie. 469, 540.

Choosing the smallest nonsquare

$469 \leq \frac{p-1}{2}$

$469^2 + 1^2 = \underbrace{218}_{m} p$, $\alpha = 469 + i$, $\beta = 33 + i$

$469 \equiv 33 \mod 218$

$1 \equiv 1 \mod 218$

~~m~~ $\gamma = \alpha\bar{\beta} = (469+i)(33-i) = 15478 - 436i = $ ~~218~~ $(71 - 2i)$

$\gamma = 71 - 2i$

$\gamma\bar{\gamma} = 71^2 + 2^2 = 5045 = 5p$

Repeat the descent step starting with $71^2 + 2^2 = \underbrace{5}_{m}p$, $\alpha = 71 + 2i$, $\beta = 1 + 2i$ mod m

$m\gamma = \alpha\bar{\beta} = (71+2i)(1-2i) = 75 - 140i = 5(15 - 28i)$

$\gamma = 15 - 28i$

$\gamma\bar{\gamma} = 15^2 + 28^2 = 1009 = p$

Which positive integers have the form a^2+b^2 $(a,b \in \mathbb{Z})$?

We know the answer for a prime number p: p is a sum of two squares iff $p=2$ or $p \equiv 1 \bmod 4$. For general n, $n = 2^{k_1} 3^{k_2} 5^{k_3} 7^{k_4} 11^{k_5} 13^{k_6} 17^{k_7} \cdots$ (all exponents are zero eventually)

eg. $n = 2^5 3^4 5^3 7^3 11^4 13^1 17^0 19^2 23^0 29^0 31^0 37^0 \cdots$ $= 2^5 \cdot 3^4 \cdot 5^3 \cdot 7^6 \cdot 11^4 \cdot 13 \cdot 19^2$ is a sum of two squares.

2^5: 2^*; 3^4: 9^2+0^2; 5^3: 5^*; 7^6: $(7^3)^2 = (7^3)^2 + 0^2$

If the exponent on every prime $\equiv 3 \bmod 4$ is even, then n is a sum of two squares; the converse is true, if some prime $p \equiv 3 \bmod 4$ has odd exponent, n cannot be a sum of two squares.

21 is not a sum of two squares. (0, 1, 4, 9, 16 are the only squares < 21)
"3·7". This can all be proved using the idea presented in the previous class.

In order to be able to write n as a sum of two squares, it needs to be small enough or we need to know its prime factorization.

Writing a number as a sum of two squares is as hard as integer factorization. Factorization in $\mathbb{Z}[i]$ is the same problem as writing a number as a sum of two squares.

Next: Public Key Cryptography, especially
- Diffie-Helman
- RSA (Rivest-Shamir-Adleman)

First: primitive elements in finite fields

Let p be prime, $\mathbb{F}_p$ = field of order p = $\mathbb{Z}/p\mathbb{Z}$ = $\{0, 1, 2, \dots, p-1\}$.

Fact: $\mathbb{F}_p$ has a <u>primitive element</u> $g \in \mathbb{F}_p$, namely all nonzero elements of $\mathbb{F}_p$ are powers of g, i.e. $\mathbb{F}_p = \{0, 1, g, g^2, g^3, \dots, g^{p-2}\}$ ($g^{p-1} = 1$ by Fermat's Little Theorem).

e.g. $\mathbb{F}_7$ has 3 as a primitive element: $\mathbb{F}_7 = \{0, 1, 3, 3^2, 3^3, 3^4, 3^5\}$, where $3^2 = 2$, $3^3 = 6$, $3^4 = 4$, $3^5 = 5$.

Also $5 = 3^{-1}$ is also a primitive element of $\mathbb{F}_7$: $\mathbb{F}_7 = \{0, 1, 5, 5^2, 5^3, 5^4, 5^5\}$, where $5^2 = 4$, $5^3 = 6$, $5^4 = 2$, $5^5 = 3$.

2 is not primitive: powers of 2 are 1, 2, 4 only.

More generally, for every prime power $q = p^k$, p prime, $k \geq 1$. $\mathbb{F}_q$ (field of order q) always has a primitive element.

Why? $\mathbb{F}_5$ has multiplicative group $\mathbb{F}_5^\times = \{1, 2, 3, 4\}$ which cannot be a Klein 4-group, otherwise $a^2 = 1$ for every nonzero $a \in \mathbb{F}_5$ but then $x^2 - 1$ is a polynomial of degree 2 having four roots in $\mathbb{F}_5$.

So $\mathbb{F}_5^\times$ must be cyclic.

eg. $\mathbb{F}_{1009} = \{0, 1, 2, \ldots, 1008\} = \{0, 1, 11, 11^2, 11^3, \ldots, 11^{1007}\}$
$= \{0, 1, 11, 121, 322, 515, 620, \ldots, 367\}$

1009 is prime

11 is a primitive (I checked using Mathematica)

$11^k = 186$ k is the "discrete logarithm" of 186 (base 11) not $\log_{11} 186 = \frac{\ln 186}{\ln 11}$

Answer: $k = 543$

$11^{543} = 186$ in $\mathbb{F}_{1009}$ i.e. in $\mathbb{Z}$, $11^{543} \equiv 186 \bmod 1009$.

Discrete logs and integer factorization are two difficult computational tasks. That's good! since this provides a secure cryptosystem for key exchange.

Alice and Bob want to agree on a large integer to be used as the encryption key for a Word document (or other symmetric key encryption algorithm) ("symmetric" means that the decryption key is the same as the encryption key).

Diffie-Hellman Key exchange protocol: Alice and Bob communicate over an open (insecure) channel. They first agree on a large prime p. (Eg. Alice can generate p and send it to Bob over the open channel.) Next, they agree on a primitive element g for $\mathbb{F}_p$. (A random element is almost as good.) One party can obtain g and send it to the other party.

Alice chooses $a \in \{2, 3, \ldots, p-2\}$ randomly and she computes $g^a \bmod p$. She sends this to Bob.
Bob chooses $b \in \{2, 3, \ldots, p-2\}$ " and he " $g^b \bmod p$. He sends this to Alice.

Eve (an eavesdropper) knows $p, g, g^a \bmod p, g^b \bmod p$; (But not a, b.)
Public key

The shared secret key is $g^{ab} \bmod p$.

Alice computes $(g^b)^a \equiv g^{ab} \bmod p$.

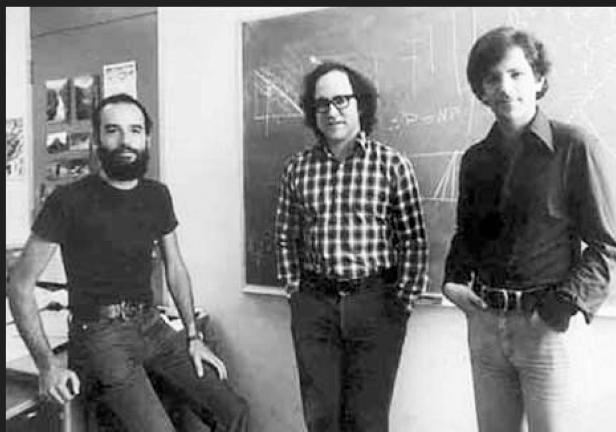
Bob computes $(g^a)^b \equiv g^{ab} \bmod p$.

Fair Coin Flip

Alice generates p, q primes generated randomly but $\begin{cases} p \equiv q \equiv 1 \mod 4 \\ \text{or} \\ p \equiv q \equiv 3 \mod 4 \end{cases}$ if a coin flip is H / " " " " " T

Alice sends $n = pq$ to Bob. $n \equiv 1 \mod 4$.

Bob guesses H or T. Bob verifies $n \equiv 1 \mod 4$, prime.



Rivest, Shamir and Adleman

inventors of the RSA encryption scheme

RSA Encryption Scheme for security and authentication over an open (insecure) channel. (Public key cryptosystem)

Alice and Bob want to communicate securely over an open channel.

Alice generates a public encryption key (n, e) as follows:

She generates two large primes p, q (each a few hundred digits long) randomly and she computes $n = pq$. She computes $\phi(n) = \phi(p)\phi(q) = (p-1)(q-1)$. She picks $e \in \{2, 3, \ldots, \phi(n)\}$ relatively prime to $\phi(n)$. Alice publishes (n, e) on her website.

Easy fact: Anyone who knows n and $\phi(n)$ can easily factor n. So keep $\phi(n), p, q$ secret!

Alice computes d = inverse of e mod $\phi(n)$, computed using the Extended Euclidean Algorithm.

Bob wants to send an integer $m \in \{1, 2, \ldots, n-1\}$ to Alice in an encrypted form so that an eavesdropper will not be able to recover the message m but Alice can decrypt.

Bob first computes $m' \equiv m^e \bmod n$. ← obtained from Alice's website. Bob sends m' to Alice.

Alice receives m' and computes $(m')^d \equiv m \mod n$.

Why does this formula hold, allowing Alice to recover m?

$$de \equiv 1 \mod \phi(n)$$

$$\Rightarrow de = 1 + k\phi(n) \text{ for some positive integer } k.$$

$$(m')^d \equiv (m^e)^d = m^{de} = m^{1+k\phi(n)} = m \cdot (m^{\phi(n)})^k \equiv m \cdot 1^k \equiv m \mod n.$$

$m^{\phi(n)} \equiv 1 \mod n$ by Euler's Formula

This assumes $\gcd(m, n) = 1$.

$\gcd(m, n) \in \{1, p, q\}$ but p, q are practically never found by chance.

Authentication : means of certifying the authenticity of a document (authorship etc.)

Security : When Bob sends a message to Alice, no one else can decrypt it (except Alice).

Authentication : " " " " " " " " Alice knows that this message actually came from Bob and it has not been altered.

PGP = Pretty good privacy

Every party generates their own RSA keys.

Alice has public key (n_A, e_A) and private key $p, q, \phi(n), d_A$

Bob has public key (n_B, e_B), " " " " d_B

Carol has public key (n_C, e_C), " " " " d_C

David " . . . .

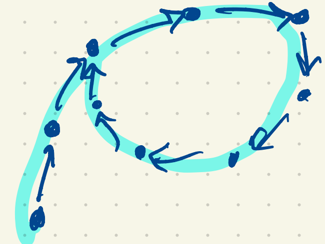
Bob wants to send Alice a message m with both secrecy and authentication capability (no one else can understand the message; and Alice has proof that the message actually came from Bob.)

Bob first computes $m' \equiv m^{d_B} \bmod n_B$ and then $m'' \equiv (m')^{e_A} \bmod n_A$. He sends m'' to Alice.

Alice receives m'' from Bob and she computes $m' \equiv (m'')^{d_A} \bmod n_A$ and $m \equiv (m')^{e_B} \bmod n_B$.

Factorization of Integers

- naive algorithm
- rho method (ρ)



Eg. Factor $n = 27641 = pq$

Look for integers x, y such that $x^2 \equiv y^2 \mod n$.

$$(x+y)(x-y) = x^2 - y^2 \text{ is divisible by } n = pq$$

$(x+y)$ divisible by $p = \gcd(n, x+y)$; $(x-y)$ divisible by $q = \gcd(n, x-y)$

Pick $a \in \{2, \dots, n-1\}$ randomly.

The map $f(a) \equiv a^2 \mod n$ can be iterated yielding a sequence $a, f(a), f(f(a)), f(f(f(a))), \dots$

For $n = 27641$, $a = 2$, we obtain the sequence (which must eventually repeat)

$$2 \to 4 \to 16 \to 256 \to 10254 \to 25793 \to 15261 \to 22696 \to 18381 \to 5218 \to 1139 \to 25835 \to 27639 \to 4$$

This gives $x = 27639$, $y = 2$ satisfying $x^2 \equiv y^2 \equiv 4 \mod n$

$$3 \to 9 \to 81 \to 6561 \to 9689 \to 21584 \to \cdots \to 21915 \to 4850 \to 9$$

gives another solution $x = 4850$, $y = 3$ with $x^2 \equiv y^2 \equiv 9 \mod n$.

$\gcd(n, 27639+2) = 211$
$\gcd(n, 27639-2) = 131$

$n = 131 \times 211$ is the prime factorization of n.

$p = 2003$ is prime. $p \equiv 3 \mod 4$.

Pick $a \in \{1, 2, \cdots, 2002\}$ randomly. 1999 $\left(\frac{1999}{2003}\right) = \left(\frac{-4}{2003}\right) = \underbrace{\left(\frac{-1}{2003}\right)}_{=-1}\underbrace{\left(\frac{4}{2003}\right)}_{=1} = -1$

Again: try $a = 990$, $\left(\frac{a}{p}\right) = -1$

Again: try $a = 824$, $\left(\frac{a}{p}\right) = 1$: 824 is a square mod $p = 2003$.

So the polynomial $x^2 - 824$ has two roots mod $p = 2003$. What are they?

$$824^{\frac{p-1}{2}} \equiv 1 \mod p \quad \text{(Euler's Criterion)}$$

$$824^{1001} \equiv 1 \mod p.$$

$$(824^{501})^2 \equiv 824^{1002} \equiv 824$$

$$824^{501} \equiv 1909 \mod p$$

In $\mathbb{F}_{2003}$, $\sqrt{824} = \pm 94$ i.e. $\sqrt{824} \in \{94, 1909\}$

When $p \equiv 1 \mod 4$, finding square roots are a little trickier. If $p = 1009$

$$\left(\frac{a}{1009}\right) = 1 \quad \text{then} \quad a^{\frac{1009-1}{2}} \equiv 1 \mod 1009$$

$$a^{504} \equiv 1 \mod p$$

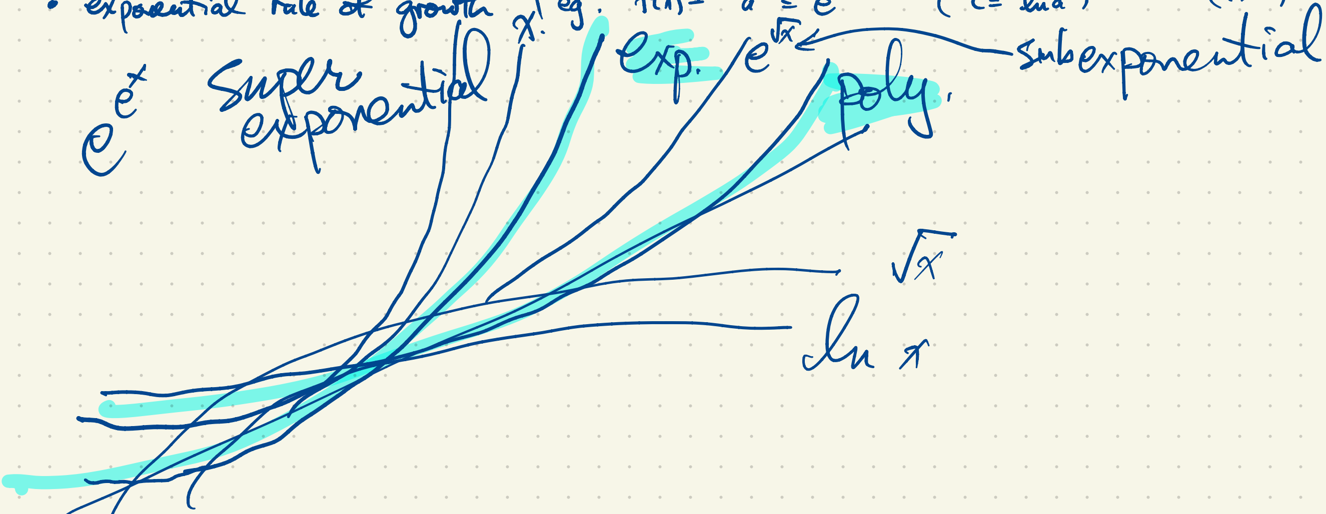
$$(\ ?\ )^2 \equiv a^{505} \equiv a \mod p$$

But square roots mod p can be efficiently computed for every p.

For functions f "going to infinity" in the sense that $\lim_{x\to\infty} f(x) = \infty$, we compare rates of growth

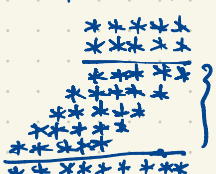
eg. • polynomial rate of growth eg. $f(x) = ax^n +$ lower degree terms, $a>0$, $n\geq 1$

• exponential rate of growth eg. $f(x) = a^x = e^{cx}$ ($c = \ln a$) $(a>1)$



Multiplication of positive integers is efficiently implemented by computer in the sense that it takes "polynomial time". Factorization is not(*) poly. time; historically it was "exponential time" but now we have "subexponential time" algorithm.

(*) Caveats: Based on current state-of-the-art knowledge.



multiply two five-digit numbers

n^2 simple multiplications + additions

At most n^3 operations to multiply two n-digit numbers.

Or n^c, $2<c<3$. The algorithm to multiply two n-digit numbers x, y runs in execution time which is polynomial in $n \approx \log x, \log y$

Naive factorization method: trial division. Given x of length $n = \log x$ digits,
try $d = 1, 2, 3, 4, \dots, \lfloor\sqrt{x}\rfloor$ until we find a divisor of x:
If none of these values divide x, return "x is prime".
Else print "d is a divisor of x so x is composite."

This requires testing $d \le \sqrt{x}$; numbers having at most $\frac{n}{2}$ digits.
How many steps? $\sqrt{x} = 10^{n/2}$ (exponential number of steps: $10^{n/2}$ is an exponential function of n.

The first factorization method running in better than exponential time is the CFRAC (Continued Fraction Method). Subexponential time.

Looking for integer solutions of

$$x^2 - 91y^2 = \pm 1$$

$$\frac{x}{y} \approx \sqrt{91}$$

$$\left(\frac{x}{y}\right)^2 - 91 = \boxed{\pm\frac{1}{y^2}}$$

Eg. Factor 91.

$$\sqrt{91} = [9,1,1,5,1,5,1,1,18,1,1,\dots] = 9 + \cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{5+\cfrac{1}{1+\cfrac{1}{5+\cdots}}}}}$$

gives a sequence of rational numbers converging to $\sqrt{91}$:

$[9] = \frac{9}{1}$ — $9^2 - 91\cdot 1^2 = -10$

$[9,1] = 9 + \frac{1}{1} = \frac{10}{1}$ — $10^2 - 91\cdot 1^2 = 9$ — $10^2 \equiv 3^2 \mod 91$

$[9,1,1] = 9 + \frac{1}{1+\frac{1}{1}} = \frac{19}{2}$ — $19^2 - 91\cdot 2^2 = -3$

$[9,1,1,5] = 9 + \frac{1}{1+\frac{1}{1+\frac{1}{5}}} = \frac{105}{11}$ — $105^2 - 91\cdot 11^2 = 14$

etc.

$\vdots$

$1574^2 - 91\cdot 165^2 = 1$

$\gcd(91, 10+3) = 13$

$\gcd(91, 10-3) = 7$

$$\left.\begin{aligned} 19^2 - 91\cdot 2^2 &= -3 \\ 124^2 - 91\cdot 13^2 &= -3 \end{aligned}\right\}$$

$(19\cdot 124)^2 \equiv 3^2 \mod 91$

$19^2\cdot 124^2 \equiv (-3)^2 \equiv 9 \equiv 3^2 \mod 91$

$x = 19\cdot 124$

$y = 3$

$x^2 \equiv y^2 \mod n$

We use linear algebra to find products giving a perfect square on the right hand side e.g.

eg.

$$x_1^2 \equiv -2 \mod n \qquad -2 = (-1)^1 2^1 3^0 5^0 7^0 11^0 \cdots \longrightarrow (1, 1, 0, 0, 0, 0, \cdots)$$

$$x_2^2 \equiv 6 \mod n \qquad 6 = (-1)^0 2^1 3^1 5^0 7^0 11^0 \cdots \longrightarrow (0, 1, 1, 0, 0, 0, \cdots)$$

$$x_3^2 \equiv 15 \mod n \qquad 15 = (-1)^0 2^0 3^1 5^1 7^0 11^0 \cdots \longrightarrow (0, 0, 1, 1, 0, 0, \cdots)$$

$$x_4^2 \equiv -5 \mod n \qquad -5 = (-1)^1 2^0 3^0 5^1 7^0 11^0 \cdots \longrightarrow (1, 0, 0, 1, 0, 0, \cdots)$$

$$(0, 0, 0, 0, 0, 0, \cdots) \quad \text{add mod } 2.$$

$$(x_1 x_2 x_3 x_4)^2 \equiv (-2)(6)(15)(-5) \mod n$$

$x = x_1 x_2 x_3 x_4$

$$\equiv (-1)^2 2^2 3^2 5^2$$

$$\equiv (-2 \cdot 3 \cdot 5)^2$$

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

Modern integer factorization

- Using a database of small primes (at most 12 digit primes) check to see if any of them divides n.
- Try elliptic curve factorization method.
- use a sieve method. These methods look for solutions of $x^2 \equiv y^2 \mod n$.

The probability that an integer chosen "randomly" in $[1,x]$ is prime is about $\frac{1}{\ln x}$ (for x large).

The actual probability is $\frac{\pi(x)}{x}$ ← number of primes in $[1,x]$; x ← number of integers in $[1,x]$

$$\sim \frac{x/\ln x}{x} = \frac{1}{\ln x} \longrightarrow 0 \quad \text{as } x \to \infty$$

What is the probability that two "randomly chosen" large integers are relatively prime?

About $0.607927 \approx 61\%$ (exactly $\frac{6}{\pi^2}$).

Buffon needle problem

The Riemann zeta function $\zeta(x) = \sum_{n=1}^{\infty} \frac{1}{n^x} = 1 + \frac{1}{2^x} + \frac{1}{3^x} + \frac{1}{4^x} + \cdots$ (convergent for $x > 1$)

$$\zeta(2) = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \frac{1}{5^2} + \frac{1}{6^2} + \cdots = \frac{\pi^2}{6}$$

$$\zeta(x) = \sum_{n=1}^{\infty} \frac{1}{n^x} = 1 + \frac{1}{2^x} + \frac{1}{3^x} + \frac{1}{4^x} + \cdots \overset{\text{claim}}{=} \prod_{p \text{ prime}} \left(\frac{1}{1-\frac{1}{p^x}}\right) = \left(\frac{1}{1-\frac{1}{2^x}}\right)\left(\frac{1}{1-\frac{1}{3^x}}\right)\left(\frac{1}{1-\frac{1}{5^x}}\right)\left(\frac{1}{1-\frac{1}{7^x}}\right)\left(\frac{1}{1-\frac{1}{11^x}}\right)\times\cdots$$

(Euler factorization)

Proof: use $\frac{1}{1-u} = 1 + u + u^2 + u^3 + u^4 + \cdots$ (geometric series)

Check: $(1-u)(1+u+u^2+u^3+\cdots) = 1 - u + u - u^2 + u^2 - u^3 + u^3 - \cdots = 1$

Harmonic Series

$\zeta(1) = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots = \infty$ (diverges)

$$\prod_p \left(\frac{1}{1-\frac{1}{p^x}}\right) = \left(\frac{1}{1-\frac{1}{2^x}}\right)\left(\frac{1}{1-\frac{1}{3^x}}\right)\left(\frac{1}{1-\frac{1}{5^x}}\right)\left(\frac{1}{1-\frac{1}{7^x}}\right)\left(\frac{1}{1-\frac{1}{11^x}}\right)\times\cdots$$

$$= \left(1 + \frac{1}{2^x} + \frac{1}{4^x} + \frac{1}{8^x} + \frac{1}{16^x} + \cdots\right)\left(1 + \frac{1}{3^x} + \frac{1}{9^x} + \frac{1}{27^x} + \cdots\right)\left(1 + \frac{1}{5^x} + \frac{1}{25^x} + \frac{1}{125^x} + \cdots\right)\left(1 + \frac{1}{7^x} + \frac{1}{49^x} + \cdots\right)\left(1 + \frac{1}{11^x} + \frac{1}{121^x} + \cdots\right)\left(1 + \frac{1}{13^x} + \frac{1}{169^x} + \cdots\right)\times\cdots$$

$$= 1 + \frac{1}{2^x} + \frac{1}{3^x} + \frac{1}{4^x} + \frac{1}{5^x} + \frac{1}{6^x} + \frac{1}{7^x} + \frac{1}{8^x} + \frac{1}{9^x} + \frac{1}{10^x} + \cdots$$

(FTA = fundamental Theorem of Arithmetic)

Given two large integers m, n, what is the probability that $\gcd(m,n)=1$ (m, n relatively prime)?

About 60.8 %, experimentally.

The probability is at most 75%, since there is a 25% chance that m, n are both even.

m, n are relatively prime iff

- m, n are not both even with probability $1-\frac{1}{4} = 75\%$
- m, n ... divisible by 3 ... $1-\frac{1}{9} = 88.8\cdots\%$
- m, n ... 5 ... $1-\frac{1}{25} = 96\%$
- m, n ... 7 ... $1-\frac{1}{49}$
- m, n ... 11 ... $1-\frac{1}{121}$

etc.

m, n are relatively prime with probability $(1-\frac{1}{4})(1-\frac{1}{9})(1-\frac{1}{25})(1-\frac{1}{49})(1-\frac{1}{121})(1-\frac{1}{169})\times\cdots = \prod_{p \text{ prime}}(1-\frac{1}{p^2}) = \frac{1}{\zeta(2)} = \frac{6}{\pi^2} \approx 0.607927\ldots$

Given three large integers l, m, n, what is the probability that they are relatively prime i.e. $\gcd(l,m,n)=1$?

e.g. $\gcd(6,10,15)=1$. This occurs with probability $\approx 83.2\%$

$$\prod_p \left(1-\frac{1}{p^3}\right) = \frac{1}{\zeta(3)} \approx 0.832$$

The probability that k large integers $m_1, \ldots, m_k$ (chosen independently at random) are relatively prime (i.e. $\gcd(m_1,\ldots,m_k)=1$) is $\frac{1}{\zeta(k)}$.

k	$\zeta(k)$	
1	∞	
2	$1.644934\cdots$	$\leftarrow \frac{\pi^2}{6}$
3	$1.202056\cdots$	$\leftarrow$ irrational. Maybe a rational multiple of π^3? Probably not.
4	$1.082323\cdots$	$\leftarrow \frac{\pi^4}{90}$
5	$1.036927\cdots$	$\leftarrow$ irrational? Who knows...
6	$1.017343\cdots$	$\leftarrow \frac{\pi^6}{945}$
...		

A number n is <u>squarefree</u> if it's not divisible by any of the squares 4, 9, 16, 25, 36, 49, 64, 81, ...

i.e. the largest square dividing n is 1.

i.e. n is not divisible by p^2 for any prime p.

What is the probability that a large number n (chosen randomly) is squarefree?

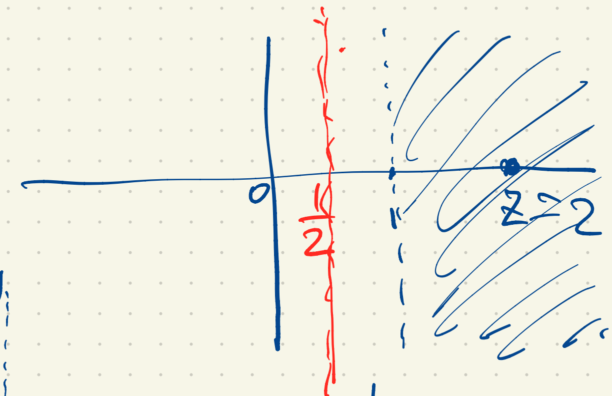
$$\frac{1}{\zeta(2)} = \frac{6}{\pi^2} \approx 0.608.$$

The Prime Number Theorem (PNT) is proved using the Riemann zeta function.

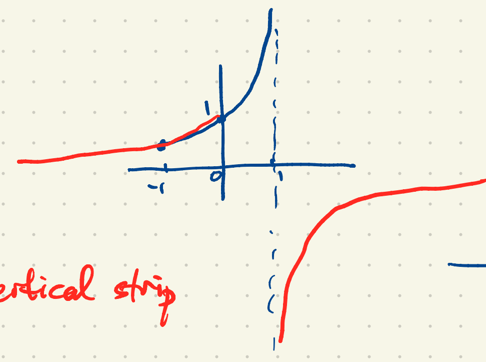
The key property of $\zeta(x)$ that yields our proof of PNT concerns where $\zeta(x) = 0$.

Much more can be said about the importance of $\zeta(x)$.

$$\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z} = 1 + \frac{1}{2^z} + \frac{1}{3^z} + \frac{1}{4^z} + \frac{1}{5^z} + \cdots \quad \text{converges for } \operatorname{Re} z > 1$$

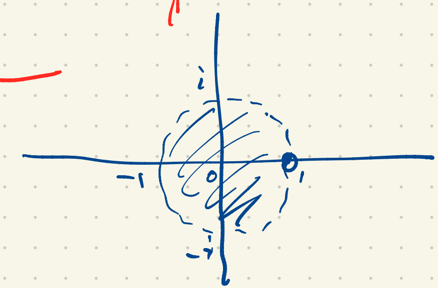


Critical line $\operatorname{Re} z = \frac{1}{2}$ i.e. $z = \frac{1}{2} + it$, $t \in \mathbb{R}$



$f(x) = 1 + x + x^2 + x^3 + x^4 + \cdots$ converges for $|x| < 1$

Actually $f(x) = \frac{1}{1-x}$



Riemann Hypothesis: The only places in the vertical strip $0 < \operatorname{Re} z < 1$ where $\zeta(z) = 0$ have $\operatorname{Re} z = \frac{1}{2}$.

$$\pi(x) = \frac{x}{\ln x} + \text{"smaller terms"}$$

Why should we care about the Riemann Hypothesis?

eg. Give a deterministic non-conditional poly. time algorithm for finding a nonsquare mod p where p is a prime.

Dirichlet's Theorem on Primes in Arithmetic Progressions

eg. There are infinitely many primes $\equiv 1 \bmod 4$. (1, 5, 9, 13, 17, 21, 25, 29, 33, ... has infinitely many primes)

There are infinitely many primes $\equiv 3 \bmod 4$. (3, 7, 11, 15, 19, 23, 27, 31 ... has infinitely many primes) (arithmetic progression)

More generally, if $\gcd(a, m) = 1$ (a, m positive integers) then the sequence $a, a+m, a+2m, a+3m, \dots$ contains infinitely many primes.

Proof uses Dirichlet L-functions (modified ζ functions)

We actually prove much more:

$$\sum_{p \text{ prime}} \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \frac{1}{17} + \frac{1}{19} + \frac{1}{23} + \cdots$$ diverges (Euler) $\Rightarrow$ There are infinitely many primes.

$$\sum_{n=1}^{\infty} \frac{1}{n} = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \cdots$$ diverges

$$\sum_{k=0}^{\infty} \frac{1}{2^k} = 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \frac{1}{32} + \frac{1}{64} + \cdots$$ Converges.

Dirichlet proved

$$\sum_{\text{primes } p \equiv 1 \bmod 4} \frac{1}{p} = \frac{1}{5} + \frac{1}{13} + \frac{1}{17} + \frac{1}{29} + \cdots$$ diverges.

$$\sum_{\text{primes } p \equiv 3 \bmod 4} \frac{1}{p} = \frac{1}{3} + \frac{1}{7} + \frac{1}{11} + \frac{1}{19} + \frac{1}{23} + \cdots$$ diverges.