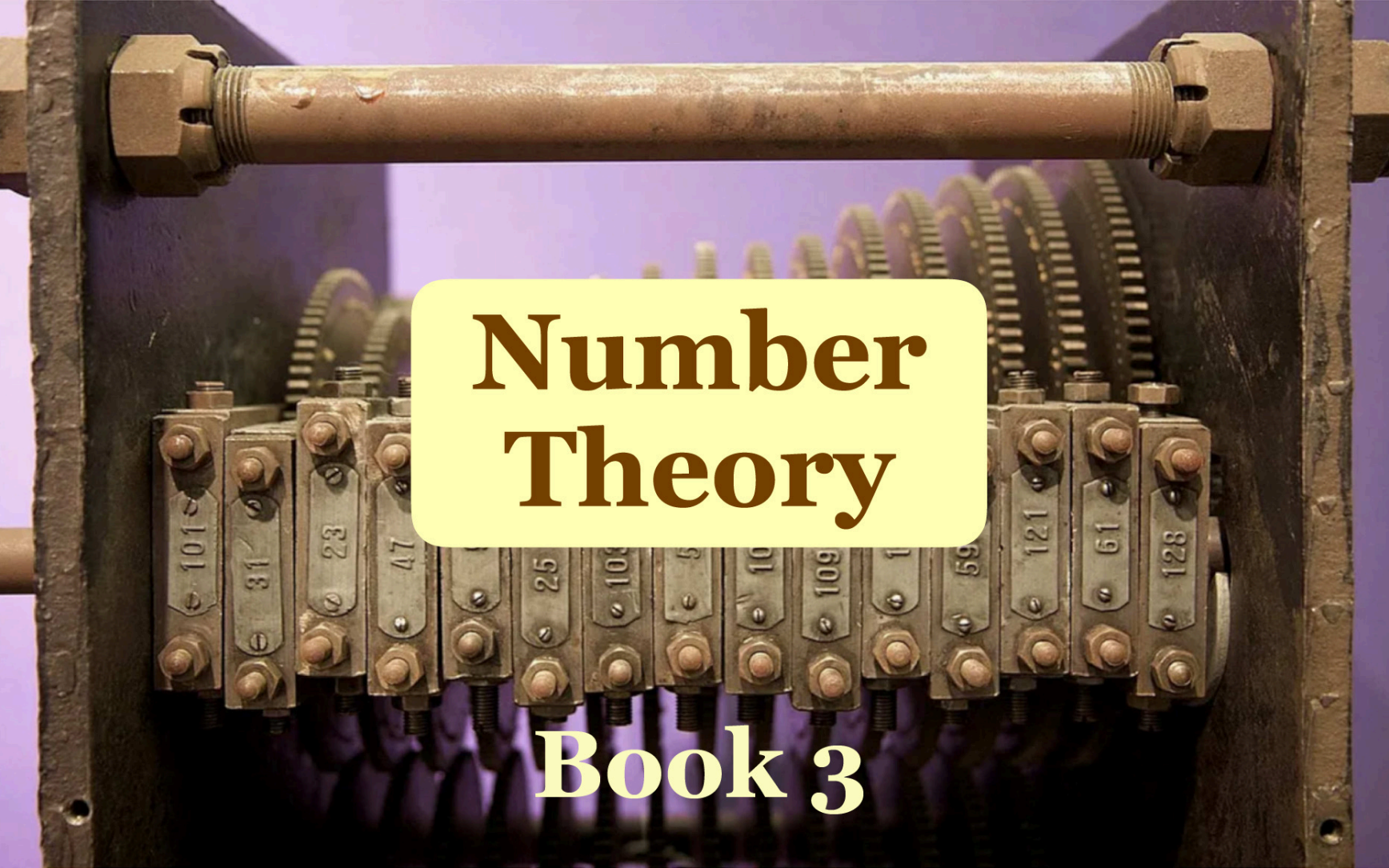

Number
Theory
Book 3

Theorem Let p be an odd prime. Then

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

Roots: all (nonzero) squares in $\mathbb{F}_p$

Roots: all nonsquares in $\mathbb{F}_p$

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,

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

Eg. is 7 a square or a nonsquare in $\mathbb{F}_{13}$? Use Euler's Criterion: $7^6 \equiv 10^3 \equiv 1000 \equiv 12 \equiv -1 \bmod 13$
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 $\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is nonzero square mod } p; \\ -1 & \text{if " " nonsquare mod } p; \\ 0 & \text{if } a \equiv 0 \bmod p. \end{cases}$

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

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

$\underbrace{\quad}_{-1} \quad \underbrace{\quad}_{+1} \quad \underbrace{\quad}_{-1}$

When is $-1 \equiv +1$ a square mod p? -1 is a { nonsquare mod $3, 7, 11, \ldots, 2003, \ldots$; square mod $5, 13$

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

Theorem 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 $\left(\frac{a}{p}\right)$:

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

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:

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

$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ 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 $\left(\frac{14}{47}\right) = \left(\frac{2}{47}\right)\left(\frac{7}{47}\right) = \left(\frac{7}{47}\right) = -\left(\frac{47}{7}\right) = -\left(\frac{5}{7}\right) = -(-1) = 1$ i.e. 14 is a square mod 47.

$\left(\frac{2}{47}\right) = +1$ since $47 \equiv -1 \bmod 8$

Since $7 \equiv 47 \equiv 3 \bmod 4$

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

$\left(\frac{2}{89}\right) = +1$ $\quad 89 \equiv 1 \bmod 4$ $\quad$ 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 $c \in \{1, \cdots, p-1\}$ 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 $a', b' \in \{-\frac{m}{2}, \cdots, \frac{m}{2}\}$ or $\{\frac{-m+1}{2}, \cdots, \frac{m-1}{2}\}$)

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

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

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

$\alpha\bar{\alpha} = mp$
$\alpha\bar{\alpha}\beta\bar{\beta} = mp\beta\bar{\beta}$
$(\alpha\bar{\beta})(\bar{\alpha}\beta) = mp\beta\bar{\beta}$
$m\gamma \cdot m\bar{\gamma} = mp\beta\bar{\beta}$
$m\,\gamma\bar{\gamma} = p\beta\bar{\beta}$
$mpk = p\beta\bar{\beta}$

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

$mk = \beta\bar{\beta}$
$m^2\gamma\bar{\gamma} = mp\beta\bar{\beta} = mp \cdot mk$
$\gamma\bar{\gamma} = pk$ 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 $p = 1009$.

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

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

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

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

Choosing the smallest nonsquare

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

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

$469 \equiv 33 \mod 218$

$1 \equiv 1 \mod 218$

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

$\gamma = 71 - 2i$

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

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

2^* $\quad 9^2+0^2$ $\quad 5^*$ $\quad (7^3)^2=(7^3)^2+0^2$

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)

"$3\cdot 7$". 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-Hellman
- RSA (Rivest-Shamir-Adleman)

First: primitive elements in finite fields

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

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

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

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

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 $a \in \mathbb{F}_5$ of degree 2 having four roots in $\mathbb{F}_5$. but then $x^2 - 1$ is a polynomial

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

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

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 $\mathbb{Z}$, $11^{543} \equiv 186 \mod 1009$.

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

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

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

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

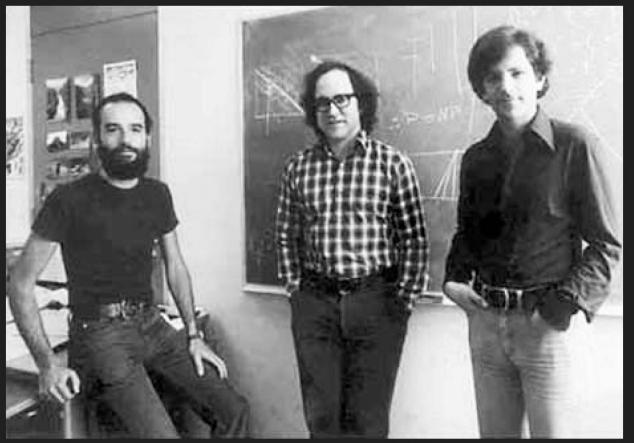
Bob computes $(g^a)^b \equiv g^{ab} \mod p$.

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.
Bob guesses H or T.

$n \equiv 1 \mod 4$.
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 $e \in \{2, 3, \dots, \phi(n)\}$ 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 $m \in \{1, 2, \dots, n-1\}$ 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 $m' \equiv m^e \bmod n$. (e, n obtained from Alice's website.) Bob sends m' to Alice.

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

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

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

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

$$(m')^d \equiv (m^e)^d = m^{de} = m^{1+k\phi(n)} = m \cdot \underbrace{(m^{\phi(n)})^k}_{m^{\phi(n)} \equiv 1 \bmod n \text{ by Euler's Formula}} \equiv m \cdot 1^k \equiv m \bmod n.$$

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

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