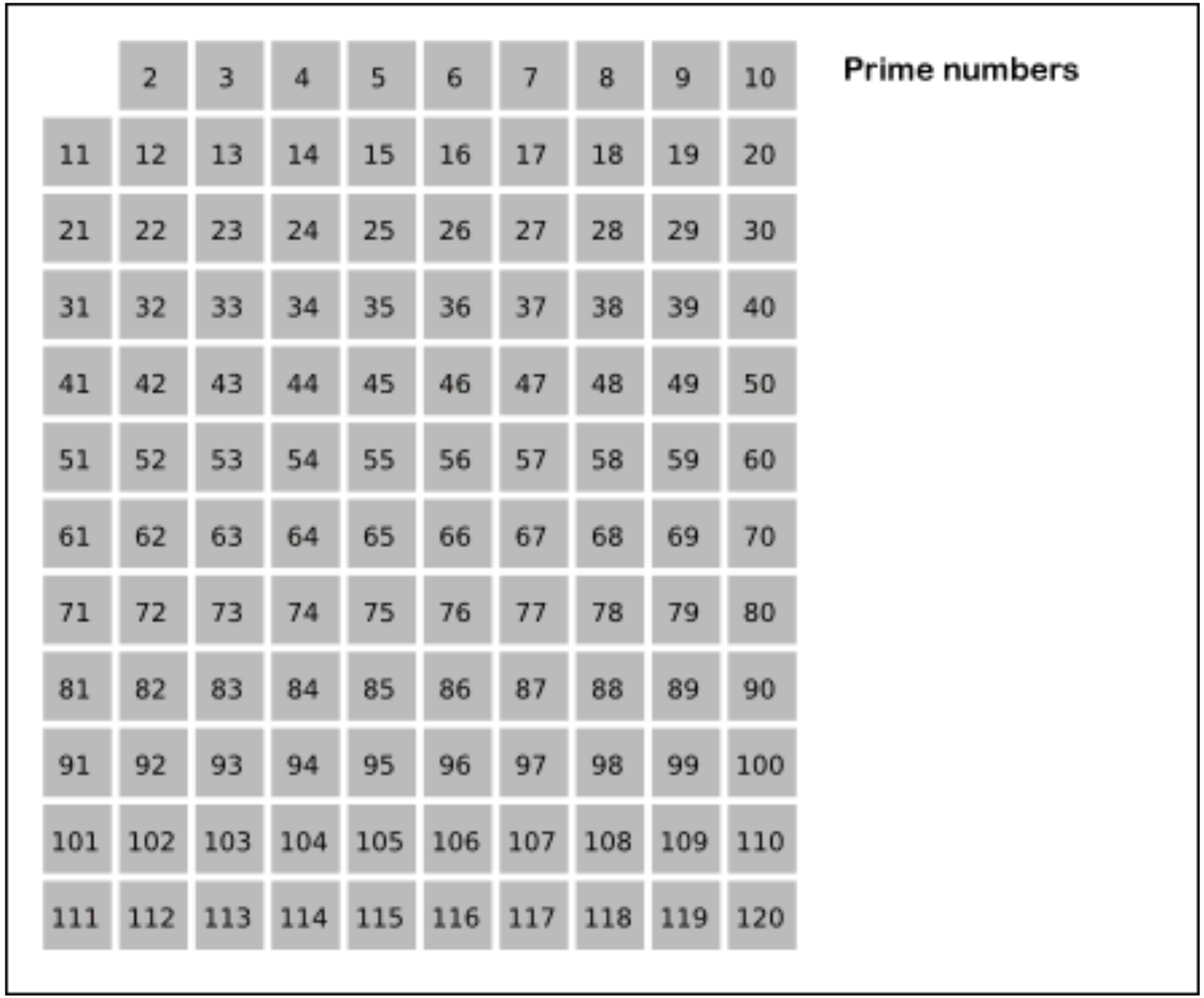
Lesson 10
Primality tests

UNIT 1
Prime numbers

The Sieve of Erastothenes



Prime number theorem

DEFINITION For any $n \geq 2$,

$$\pi(n) = \#\{p : \ p \text{ prime}, 2 \leq p \leq n\}$$

```
In[385]:= PrimePi[130]
Out[385]= 31
```

THEOREM (the Prime number Theorem)

$$\lim_{n \to +\infty} \frac{\pi(n)}{n/\log n} = 1$$

EXAMPLE **How many primes do you expect between 900 000 and 1 000 000?**

$$\pi(1\,000\,000) - \pi(900\,000) \approx \frac{1\,000\,000}{\log(1\,000\,000)} - \frac{900\,000}{\log(900\,000)} \approx 6737.$$

Actually (Mathematica), there are 7224 prime numbers in that interval.

Prime number theorem

EXAMPLE

In cryptography one needs primes with around 1024 bits

($2^{1024} \approx 10^{308.25}$: about 300 decimal digits)

How many primes between 2^{1023} and 2^{1024}?

$$\pi(2^{1024}) - \pi(2^{1023}) \approx \frac{2^{1024}}{\log(2^{1024})} - \frac{2^{1023}}{\log(2^{1023})}$$

$$\approx 2^{1013.53}: \quad \text{a lot!}$$

Notice that the probability of finding a prime in $[2^{1023}, 2^{1024}]$ is

$$\approx \frac{2^{1013.53}}{2^{1024} - 2^{1023}} = \frac{2^{0.53}}{2^{11} - 2^{10}} \approx 0.014\%$$

Prime number theorem

COROLLARY

The probability that a number in $2, \ldots, n$ is prime is asymptotic to $\frac{1}{\log n}, n \to +\infty$.

Meaning: fix $c_1, c_2 > 0$. **Let $P(n) := \frac{\#\text{primes in } [c_1 n, c_2 n]}{c_2 n - c_1 n}$.**

Then $\lim_{n \to +\infty} \frac{P(n)}{1/\log n} = 1$. Equivalently: $\pi(n) = \frac{n}{\log n} + o\left(\frac{n}{\log n}\right), n \to +\infty$.

Proof.

$$(c_2 n - c_1 n) P(n) = \pi(c_2 n) - \pi(c_1 n) = \frac{c_2 n}{\log(c_2 n)} - \frac{c_1 n}{\log(c_1 n)} + o\left(\frac{n}{\log n}\right)$$

Now $\frac{n}{\log(cn)} = \frac{n}{\log c + \log n} \sim \frac{n}{\log n}, n \to +\infty$.

Thus $(c_2 n - c_1 n) P(n) = \frac{(c_2 - c_1) n}{\log n} + o\left(\frac{n}{\log n}\right) \sim \frac{(c_2 - c_1) n}{\log n}, n \to +\infty$. □

The Riemann hypothesis

The Riemann zeta function on $s > 1$.

For $s > 1$, s real: $$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Relation with prime numbers. **For $s > 1$,** $$\zeta(s) = \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right).$$

The Riemann zeta function on $\mathbb{C} \setminus \{1\}$.

It can be extended to a holomorphic function in $\mathbb{C} \setminus \{1\}$ with a simple pole at 1.

$$\zeta(s) \sim \frac{1}{s-1} \text{ as } s \to 1.$$

Trivial zeroes: $-2, -4, -6, \ldots, -2n, \ldots$

Riemann hypothesis. **The only nontrivial zeros of ζ are on the line** $\frac{1}{2} + i\mathbb{R}$.

UNIT 2
Fermat (non)Primality test

Fermat (non)primality test

RECALL (Fermat, version 2) **Let p be a prime. Then**

$$\forall a \in \mathbb{Z} \qquad a^p \equiv a[p]$$

Proof. **If $p \nmid a$ then $a^{p-1} \equiv 1[p]$ (Fermat). If $p \mid a$ then $a^p \equiv 0 \equiv a[p]$.** $\square$

COROLLARY [Fermat (non)primality test]

Let $n \in \mathbb{N}, n \geq 2$. If $a \in \mathbb{Z}$ is such that $a^n \not\equiv a[n]$ then n is not prime.

DEFINITION **Let $n \in \mathbb{N}_{\geq 2}$. An integer a is a (Fermat) witness for n if $a^n \not\equiv a[n]$.**

Witnesses for Fermat test

***a* witness for *n*: *a* satisfies Fermat test [*n*]:** $a^n \not\equiv a[n]$

***a* not witness for *n*:** $a^n \equiv a[n]$

REMARK **Reformulation: if n has a witness then n is not prime.**

REMARK $a^{n-1} \equiv 1[n] \Rightarrow a^n \equiv a[n]$.

Converse is false: $4^{11} \equiv 4 \not\equiv 1[12], 4^{12} \equiv 4[12]$

If $\gcd(a, n) = 1$ then $a^n \equiv a[n] \Leftrightarrow a^{n-1} \equiv 1[n]$.

Witnesses for Fermat test

REMARK **Checking a WITNESS is MUCH EASIER THAN finding PRIME FACTORS!**

Check if a has prime divisors: $O(\sqrt{n})$ steps.

Check if a is a witness for n: compute a^n: $O(\log n)$ steps.

EXAMPLE $n = 319879377374793553326200686437131014909523353 01.$

- **n is not divisible by primes smaller than $1\,000\,000$. Is n prime?**
- $2^n \equiv 319879377374793553326200686437131014909523353 01 \not\equiv 2[n]$: **n not prime.**

Witnesses for Fermat test

EXAMPLE $n = 209$. Check whether 2 is a witness for n.

$\gcd(2, 209) = 1$: need to compute $2^{208}[209]$.

We need to compute $2^{208}[209]$:

Witnesses for Fermat test

EXAMPLE **Is 30069476293 a prime number?**

Fermat (non)primality test

EXAMPLE We want to find the first $k \geq 1$ such that $n(k) = 10^{22} + k$ is prime.

We exclude k even and multiples of 5.

Among these k find the first k such that 2 is not a witness for $n(k)$:

$\gcd(2, 10^{22} + k) = 1$: need to check if $2^{n(k)-1} \not\equiv 1[n(k)]$.

k	1	3	7	9
$2^{n(k)-1}[n(k)]$	*385214351462115178459 1*	*246729341461766517323 3*	*753393392967616725845 6*	**1**

Is $n(9) = 10^{22} + 9$ prime?

Try $a = 3$: $3^{n(9)} \equiv 3[n(9)]$

Try $a = 4$: $4^{n(9)} \equiv 4[n(9)]$

How about if none are witnesses? Is $n(9)$ prime?

Fermat test does not prove primality

Carmichael numbers

EXAMPLE $n = 561 = 3 \times 11 \times 17$. **Claim: no witnesses for** n.

Let $a \in \mathbb{Z}$. **We prove that** $a^{561} \equiv a[561]$.

$560 = 2^4 \cdot 5 \cdot 7$

DEFINITION

NO WITNESSES for *n*

$n \in \mathbb{N}$ **is a** Carmichael **number if** n **is not prime and** $a^n \equiv a[n]$ **for all** $a \in \mathbb{Z}$.

Carmichael numbers

THEOREM (Alford, Granville, Pomerance -1994)

There are infinitely many Carmichael numbers.

REMARK

Carmichael numbers are rare:

$$\#\{1 \leq n \leq 10^{21} : n \text{ is Carmichael}\} = 20138200 \text{ (Pinch)}$$

$$\mathrm{P}(\{1 \leq n \leq 10^{21} : n \text{ is Carmichael}\}) = \frac{20138200}{10^{21}} \approx 2 \times 10^{-14}$$

UNIT 3
Fermat's alternative Theorem

Fermat's alternative

THEOREM (Fermat's alternative Theorem) No need that q is prime

Let p be an odd prime, $p-1=2^k q$, with $2 \nmid q$, $k \geq 1$. Let $a \in \mathbb{Z}$ with $p \nmid a$.

Then at least one of the conditions is true:

(i) $a_0 :\equiv a^q \equiv 1[p]$;

(ii) At least one among the successive squares

Compute squares as in the Fast Powering Algorithm

$$a_0 :\equiv a^q[p], \quad a_1 :\equiv a_0^2 = a^{2q}[p], \quad a_2 :\equiv a_1^2 = a^{2^2 q}[p] \ldots, a_{k-1} :\equiv a_{k-2}^2 \equiv a^{2^{k-1}q}[p]$$

is congruent to $-1[p]$.

REMARK If $p \mid a$: $a_0 \equiv a_1 \equiv \cdots \equiv a_{k-1} \equiv 0[p]$

REMARK It implies little Fermat's THM:

actually the proof of the alternative THM requires little Fermat...

$$a^q \equiv 1[p] \Rightarrow a^{p-1} = (a^q)^{2^k} \equiv (1)^{2^k} = 1[p]$$

$$a^{2^i q} \equiv -1[p], i \leq k-1 \Rightarrow a^{p-1} = \left(\left(a^{2^i q}\right)^{2^{k-1-i}}\right)^2 \equiv 1[p].$$

Fermat's alternative

REMARK **Given N odd, how to find k, q such that $N - 1 = 2^k q, 2 \nmid q$?**

Divide successively $N - 1$ by 2 until the quotient is no more divisible by 2:

k is the number of divisions, $q = \dfrac{N-1}{2^k}$.

A property of prime numbers

PROPOSITION (Fermat's alternative Theorem)

Let p be an odd prime, $p-1=2^k q$, with $2 \nmid q$. Let $a \in \mathbb{Z}$ with $p \nmid a$.

No need that q is prime

Then one of the conditions is true:

(i) $a_0 :\equiv a^q \equiv 1[p]$;

(ii) At least one among the successive squares

$$a_0 :\equiv a^q[p], \quad a_1 :\equiv a_0^2 = a^{2q}[p], \quad a_2 :\equiv a_1^2 = a^{2^2 q}[p] \ldots, a_{k-1} :\equiv a^{2^{k-1}q}[p]$$

is congruent to $-1[p]$.

EXAMPLE $p = 53, p-1 = 52 = 2^2 \cdot 13 = 2^k q, k = 2, q = 13.$

- $a = 6$

A property of prime numbers

PROPOSITION (Fermat's alternative Theorem)

Let p be an odd prime, $p-1=2^k q$, with $2 \nmid q$. Let $a \in \mathbb{Z}$ with $p \nmid a$.

No need that q is prime

Then one of the conditions is true:

(i) $a_0 :\equiv a^q \equiv 1[p]$;

(ii) At least one among the successive squares

$a_0 :\equiv a^q[p], \quad a_1 :\equiv a_0^2 = a^{2q}[p], \quad a_2 :\equiv a_1^2 = a^{2^2 q}[p] \ldots, a_{k-1} :\equiv a^{2^{k-1}q}[p]$

is congruent to $-1[p]$.

EXAMPLE

$$p = 17, p-1 = 16 = 2^4 \cdot 1 = 2^k q, k = 4, q = 1.$$

Check the validity of Fermat's alternative Theorem with a = 3, 4, 8

A property of prime numbers

PROPOSITION (Fermat's alternative Theorem)

Let p be an odd prime, $p-1=2^k q$, with $2 \nmid q$. Let $a \in \mathbb{Z}$ with $p \nmid a$.

No need that q is prime

Then one of the conditions is true:

(i) $a_0 :\equiv a^q \equiv 1[p]$;

(ii) At least one among the successive squares

$$a_0 :\equiv a^q[p], \quad a_1 :\equiv a_0^2 = a^{2q}[p], \quad a_2 :\equiv a_1^2 = a^{2^2 q}[p] \ldots, a_{k-1} :\equiv a^{2^{k-1}q}[p]$$

is congruent to $-1[p]$.

EXAMPLE

$$p = 13, p-1 = 12 = 2^2 \cdot 3 = 2^k q, k = 2, q = 3.$$

Check the validity of Fermat's alternative Theorem with a = 3, 4, 5

A property of prime numbers - proof

THEOREM (Fermat's alternative Theorem): the proof

Let p be an odd prime, $p-1=2^k q$, with $2\nmid q$, $k\geq 1$. Let $a\in\mathbb{Z}$ with $p\nmid a$.

Then one of the conditions is true:

(i) $a_0 :\equiv a^q \equiv 1[p]$;

(ii) At least one among the successive squares

$$a_0 :\equiv a^q[p],\quad a_1 :\equiv a_0^2 \equiv a^{2q}[p],\quad a_2 :\equiv a_1^2 \equiv a^{2^2 q}[p]\ldots, a_{k-1} :\equiv a^{2^{k-1}q}[p]$$

is congruent to $-1[p]$.

Proof.

A property of prime numbers - a Lemma

LEMMA **Let p be a prime and $b \in \mathbb{Z}$ be such that $b^{2^k} \equiv 1[p]$ for some $k \geq 1$.**

Then one of the following possibilities may occur:

(i) $b \equiv 1[p]$;

(ii) At least one among the successive squares

$$b_0 :\equiv b[p], \quad b_1 :\equiv b^2[p], \ldots, b_{k-1} :\equiv b^{2^{k-1}}[p]$$

is congruent to $-1[p]$.

Proof. **Recall: $x^2 = 1$ in $\mathbb{F}_p \Leftrightarrow x = \pm 1$.**

A property of prime numbers - proof

THEOREM (Fermat's alternative Theorem): the proof

Let p be an odd prime, $p-1=2^k q$, with $2\nmid q$, $k\geq 1$. Let $a\in\mathbb{Z}$ with $p\nmid a$.

Then one of the conditions is true:

(i) $a_0 :\equiv a^q \equiv 1[p]$;

(ii) At least one among the successive squares

$$a_0 :\equiv a^q[p],\quad a_1 :\equiv a_0^2 \equiv a^{2q}[p],\quad a_2 :\equiv a_1^2 \equiv a^{2^2 q}[p]\ldots, a_{k-1} :\equiv a^{2^{k-1}q}[p]$$

is congruent to $-1[p]$.

Proof. **Fermat's THM** $\Rightarrow a^{p-1}\equiv 1[p]$. **Let** $b:=a^q$**: then** $b^{2^k}\equiv a^{2^k q}\equiv 1[p]$.

UNIT 4
Strong Fermat (non) Primality test

Recall: Fermat's alternative thm for prime numbers

THEOREM (Fermat's alternative Theorem)

Let p be an odd prime, $p-1=2^k q$, with $2 \nmid q$, $k \geq 1$. Let $a \in \mathbb{Z}$ with $p \nmid a$.

Then at least one of the conditions is true:

(i) $a_0 :\equiv a^q \equiv 1[p]$;

(ii) At least one among the successive squares

$$a_0 :\equiv a^q[p], \quad a_1 :\equiv a_0^2 = a^{2q}[p], \quad a_2 :\equiv a_1^2 = a^{2^2 q}[p] \ldots, a_{k-1} :\equiv a_{k-2}^2 \equiv a^{2^{k-1} q}[p]$$

is congruent to $-1[p]$.

Strong Fermat (non) primality test

COROLLARY
(Strong Fermat test: Violation of Fermat's alternative)

THEOREM (Fermat's alternative Theorem)

Let p be an odd prime, $p-1=2^k q$, with $2 \nmid q$, $k \geq 1$. Let $a \in \mathbb{Z}$ with $p \nmid a$.

Then at least one of the conditions is true:

(i) $a_0 :\equiv a^q \equiv 1[p]$;

(ii) At least one among the successive squares

$a_0 :\equiv a^q[p], \quad a_1 :\equiv a_0^2 = a^{2q}[p], \quad a_2 :\equiv a_1^2 = a^{2^2 q}[p] \ldots, a_{k-1} :\equiv a_{k-2}^2 \equiv a^{2^{k-1}q}[p]$

is congruent to $-1[p]$.

Let n be an odd integer, $n-1=2^k q$, with $2 \nmid q$, $k \geq 1$. Let $a \in \mathbb{Z}$ with $\gcd(a,n)=1$.

Often a=2

Assume that:

$k \leq \log_2 n$

(i) $a_0 :\equiv a^q \not\equiv 1[n]$;

(ii) None among the successive squares

$$a_0 :\equiv a^q[n],\ a_1 :\equiv a_0^2 = a^{2q}[n],\ a_2 :\equiv a_1^2 \equiv a^{2^2 q}[n], \ldots,\ a_{k-1} :\equiv a_{k-2}^2 \equiv a^{2^{k-1}q}[n]$$

is congruent to $-1[n]$.

Then n is NOT prime.

Such an integer a is called a strong Fermat witness or Miller-Rabin witness for n.

Strong Fermat (non) primality test

COROLLARY (Strong Fermat test)

Let n be an odd integer, $n-1=2^k q$, with $2 \nmid q$. Let $a \in \mathbb{Z}$ with $\gcd(a,n)=1$.

Assume that:

(i) $a_0 :\equiv a^q \not\equiv 1[n]$;

(ii) None among the successive squares

$$a_0 :\equiv a^q[n], \quad a_1 :\equiv a_0^2 = a^{2q}[n], \quad a_2 :\equiv a_1^2 \equiv a^{2^2 q}[n] \ldots, a_{k-1} :\equiv a^{2^{k-1}q}[n]$$

is congruent to $-1[n]$.

Then n is NOT prime. Such an integer a is called a strong witness for n.

EXAMPLE $n = 91.$

Take $a=3$. $3^{90} \equiv 1[91]$: 3 is not a witness for Fermat test.

Let's check if it is strong witness

Strong Fermat (non) primality test

EXAMPLE (Carmichael 561)

$n = 561$. Take $a = 2$: $\gcd(2, 561) = 1$.

Recall: $2^{560} \equiv 1[560]$

COROLLARY (Strong Fermat test)

Let n be an odd integer, $n - 1 = 2^k q$, with $2 \nmid q$. Let $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$.

Assume that:

(i) $a_0 :\equiv a^q \not\equiv 1[n]$;

(ii) None among the successive squares

$$a_0 :\equiv a^q[n], \quad a_1 :\equiv a_0^2 = a^{2q}[n], \quad a_2 :\equiv a_1^2 \equiv a^{2^2 q}[n] \ldots, a_{k-1} :\equiv a^{2^{k-1} q}[n]$$

is congruent to $-1[n]$.

Then n is NOT prime. Such an integer a is called a strong witness for n.

Witnesses and strong witnesses for n

(Fermat) witness	Strong (Fermat) witness
$n \geq 2$	$n \geq 2$ **odd**
$a \in \mathbb{Z}$	$a \in \mathbb{Z}, \gcd(a, n) = 1$
$a^n \not\equiv a[n]$	$n - 1 = 2^k q$, with $2 \nmid q$, $k \geq 1$. (i) $a_0 :\equiv a^q \not\equiv 1[n]$; (ii) None among the successive squares $a_0 :\equiv a^q[n]$, $a_1 :\equiv a_0^2 = a^{2q}[n]$, $a_2 :\equiv a_1^2 \equiv a^{2^2 q}[n], \ldots, a_{k-1} :\equiv a_{k-2}^2 \equiv a^{2^{k-1} q}[n]$ is congruent to $-1[n]$.

not restrictive in view of determining if n is prime

ALGORITHM (non primality)

1. a is a witness: n is not prime.
2. a is not witness: i) a is a Strong witness: n is not prime.
   ii) a is not a Strong witness: change a.

Strong Fermat (non) primality test

EXAMPLE: is 2 a strong witness for 21?

$n = 21$. Take $a = 2$: $\gcd(2, 21) = 1$.

$n - 1 = 20 = 2^2 \cdot 5$: $k = 2, q = 5$.

COROLLARY (Strong Fermat test)

Let n be an odd integer, $n - 1 = 2^k q$, with $2 \nmid q$. Let $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$.

Assume that:

(i) $a_0 :\equiv a^q \not\equiv 1[n]$;

(ii) None among the successive squares

$$a_0 :\equiv a^q[n], \quad a_1 :\equiv a_0^2 = a^{2q}[n], \quad a_2 :\equiv a_1^2 \equiv a^{2^2 q}[n] \ldots, a_{k-1} :\equiv a^{2^{k-1} q}[n]$$

is congruent to $-1[n]$.

Then n is NOT prime. Such an integer a is called a strong witness for n.

Strong Fermat (non) primality test

COROLLARY (Strong Fermat test)

Let n be an odd integer, $n-1=2^k q$, with $2 \nmid q$. Let $a \in \mathbb{Z}$ with $\gcd(a,n)=1$.

Assume that:

(i) $a_0 :\equiv a^q \not\equiv 1[n]$;

(ii) None among the successive squares

$$a_0 :\equiv a^q[n], \quad a_1 :\equiv a_0^2 = a^{2q}[n], \quad a_2 :\equiv a_1^2 \equiv a^{2^2 q}[n] \ldots, a_{k-1} :\equiv a^{2^{k-1}q}[n]$$

is congruent to $-1[n]$.

Then n is NOT prime. Such an integer a is called a strong witness for n.

EXAMPLE (existence of a Strong witness does not imply primality)

Is $a=3$ a witness for $n=121$?

Is $a=3$ a strong witness for $n=121$?

Why is it better to use the STRONG Fermat test?

Remember: a Carmichael number is a composite number that has no witnesses

There are no Carmichael-like numbers for strong Fermat test.

PROPOSITION

Let n be an odd composite number (i.e., not prime). Then at least 75% of the numbers $1 \leq a \leq n-1$ are strong witnesses for n.

$$P(\{a \in \{1, ..., n-1\} : \ a \text{ is a strong witness for } n\}) \geq 75\%$$

COROLLARY Let n be odd and composite. Choose m random values in $1, ..., n-1$. The probability that none of them is a strong witness is less than $(1/4)^m$.

Why is it better to use strong Fermat test

COROLLARY (Rabin-Miller primality test)

Take a large integer n. You perform the strong Fermat test to m random integers $1 \leq a \leq n-1$. None of them is a strong witness.

The probability that n is composite (non prime) is less than $\frac{\log n}{4^m}$.

$$P(n \text{ is composite} \mid \text{ there are } m \text{ witnesses}) \leq \tfrac{\log n}{4^m}$$

Proof. C: n is composite. F: m witnesses in $\{1, \ldots, n-1\}$.

We know that $P(F \mid C) = p \leq 1/4^m$. We need to compute $P(C \mid F)$.

$$\text{Bayes: } P(C \mid F) = \frac{P(F \mid C)P(C)}{P(F)} = \frac{P(F \mid C)P(C)}{P(F \mid C)P(C) + P(F \mid \neg C)P(\neg C)}$$

$$\neg C\text{: } n \text{ is prime. } P(\neg C) = \frac{1}{\log n}, \;\; P(F \mid C) := p \leq \frac{1}{4^m}, \;\; P(F \mid \neg C) = 1$$

$$P(C \mid F) = \frac{p\left(1 - \frac{1}{\log n}\right)}{p\left(1 - \frac{1}{\log n}\right) + \frac{1}{\log n}} \leq \frac{p\left(1 - \frac{1}{\log n}\right)}{\frac{1}{\log n}} \leq p \log n \leq \frac{\log n}{4^m}. \quad \square$$

Why is it better to use strong Fermat test

INFORMAL PROOF

Take a large integer n. You perform the strong Fermat test to m random integers $1 \leq a \leq n-1$. None of them is a strong witness.

The probability that n is composite (non prime) is less than $\dfrac{\log n}{4^m}$.

Informal Proof. **C: n is composite. F: m witnesses in $\{1, \ldots, n-1\}$.**

In average, on n integers:

	C does not occur	
	C occurs	

Complexity of primality testing

THEOREM (Miller) FAST ALGORITHM ?

If n is composite then n has a strong witness smaller than $2(\log n)^2$.

(Actually its validity depends on that of the (generalized) Riemann hypothesis)

There is a polynomial-time primality test

THEOREM (AKS Primality test, Agrawal-Kayal-Saxena, 2002) FAST ALGORITHM

For every $\varepsilon > 0$, there is an algorithm that conclusively determines wheter a given number n is prime in no more than $O\big((\log n)^{6+\varepsilon}\big)$ steps.

UNIT 5
Lucas Primality test

order mod. a natural

DEFINITION Let $n > 1$ be an integer, $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$.

The order $\mathrm{ord}_n(a)$ of a modulo n is the minimum $m \geq 1$ such that $a^m \equiv 1[n]$.

The existence of the order is ensured by Euler's theorem

PROPOSITION Let $n > 1$ be an integer, $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$.

If $a^m \equiv 1[n]$ then $\mathrm{ord}_n(a) \mid m$. In particular $\mathrm{ord}_n(a) \mid \varphi(n)$.

Proof. Similar to the one with n prime.

EXAMPLE The order of 7 mod. 18 is 3.

Indeed $7^2 \equiv 13[18], 7^3 \equiv 1[18]$.

Finding the order mod. a natural

EXERCISE **Find the order of 3 mod. 121 (without making the list of all powers).**

$\varphi(121) = \varphi(11^2) = 11(11-1) = 110.$ **The order of 3 is a divisor of 110.**

$110 = 2 \cdot 5 \cdot 11$

Its nontrivial divisors are 2, 5, 11, 10, 22, 55.

$3^2 \equiv 9 \not\equiv 1[121], 3^5 = 243 \equiv 1[121].$

Thus the order of 3 divides 5, which is prime. Thus $\mathrm{ord}_{121}(3) = 5.$

Recall: characterisation of primitive roots

RECALL: CHARACTERISATION OF PRIMITIVE ROOTS mod. a prime

Let $p > 2$ be prime and $p - 1 = \prod_{i=1}^{m} p_i^{a_i}$ be the prime decomposition of $p - 1$, with p_i distinct and $a_i \geq 1$ for $i = 1, \ldots, m$.

Then $g \in \mathbb{F}_p{}^*$ is a primitive root if and only if $g^{(p-1)/p_i} \not\equiv 1[p]$ for $i = 1, \ldots, m$.

$\Leftrightarrow$ $g^{(p-1)/q} \not\equiv 1[p]$ for every prime divisor q of $(p-1)$.

REMARK

1) $p \in \mathbb{F}_p^* \Leftrightarrow \gcd(g, p) = 1$

2) g primitive root in $\mathbb{F}_p \Leftrightarrow \mathrm{ord}_p(g) = p - 1$.

Characterisation of elements of a given order

Extension of the characterisation of primitive roots to non prime modularities.

PROPOSITION (characterisation of the elements of given order)

Let $n > 1$ be an integer, $g \in (\mathbb{Z}/n\mathbb{Z})^*$ with $\gcd(g, n) = 1$.

Let $N \geq 1$ be such that $g^N \equiv 1[n]$.

Then $\mathrm{ord}_n(g) = N$ if and only if $g^{N/q} \not\equiv 1[n]$ for every prime divisor q of N.

Proof. **Obviously if $N = \mathrm{ord}_n(g)$ then $g^{N/q} \not\equiv 1[n]$ for any prime divisor q of N.**

If $\mathrm{ord}_n(g) < N$ then $N = d\,\mathrm{ord}_n(g)$ for some $d > 1$.

Thus, if q is a prime divisor of d we have $g^{N/q} = \left(g^{\mathrm{ord}_n(g)}\right)^{d/q} \equiv 1[n]$. $\square$

Lucas Primality test

Suppose that n passes the Strong Fermat test for several values of a, so we suspect that n is prime. Again, the factorization of $n-1$ turns out to be useful.

THEOREM (Lucas) **Let $n \in \mathbb{N}, n \geq 2$. let $1 < a < n$ be such that:**

1. $a^{n-1} \equiv 1[n]$; a is a witness for n

2. $a^{(n-1)/p} \not\equiv 1[n]$ **for every prime factor p of $n-1$.**

Then n is prime.

Proof. **The assumptions are equivalent to the fact that $\mathrm{ord}_n(a) = n-1$.**

Since $\mathrm{ord}_n(a) \mid \varphi(n)$ we have $n-1 \mid \varphi(n) \leq n-1$:

thus $\varphi(n) = n-1$, i.e., n is prime. $\square$

Lucas Primality test

THEOREM (Lucas) Let $n \in \mathbb{N}, n \geq 2$. let $1 < a < n$ be such that:

1. $a^{n-1} \equiv 1[n]$;
2. $a^{(n-1)/p} \not\equiv 1[n]$ for every prime factor p of $n-1$.

Then n is prime.

EXERCISE Can we deduce that 29 is prime from Lucas primality test with $a = 2$?

Lucas Primality test

THEOREM (Lucas) Let $n \in \mathbb{N}, n \geq 2$. let $1 < a < n$ be such that:

1. $a^{n-1} \equiv 1[n]$;
2. $a^{(n-1)/p} \not\equiv 1[n]$ for every prime factor p of $n-1$.

Then n is prime.

EXERCISE Use Lucas test with $a = 11$ to check that $n = 71$ is prime.

END of
Lesson 10
Primality tests