How do you determine if a number $n$ is prime?

Check if every $x < n$ has $x \mid n$.
Check if every $x \leq \sqrt{n}$ has $x \mid n$.

If $(a,n) = 1$ and $a^{\phi(n)} \equiv 1 \pmod{n}$ then $n$ is not prime.

[Not perfect: $n = 216 = 2^3 \cdot 3^3$]

Consider $n = 3317$.

$2 \mid 3317$, $3 \mid 3317$, $4 \nmid 3317$.

$p = 16\cdot 201$.

$3317 \equiv 1 \pmod{16}$.

$3317 \equiv 1 \pmod{201}$.

$3317 \equiv 1 \pmod{11}$.

$3317 \equiv 1 \pmod{17}$.

Thus, $3317$ is prime.

A composite $n$ for which $a^{\phi(n)} \equiv 1 \pmod{n}$ is called a pseudoprime to the base $a$.

Wilson's theorem: If $p$ is prime, then $(p-1)! \equiv -1 \pmod{p}$.

Computationally one can see:

- If $p$ is prime, then $x^2 \equiv 1 \pmod{p} \Rightarrow x \equiv \pm 1$.
- If $n$ is odd, write $n-1 = 2^kd$ with $d$ odd.
- Then if $n$ is prime $a^{n-1} \equiv 1 \pmod{n}$, look at $a^d, a^{2d}, a^{3d}, \ldots, a^{kd}$ (mod $n$).
- If the last one which is not $1$ must be $-1$.
- So if $n-1 = 2^kd$ and $a^{kd} \equiv 1, a^{2kd} \not\equiv 1$ then $n$ is composite.
\[ n-1 = 2^k d \]

If \( a^{2^j d} \equiv 1 \pmod{n} \) for some \( j \leq k \), then

- \( n \) is a strong pseudoprime to \( b \) base \( a \).
- \( n \) is SPSP(\( a \)).

**Fact:** if \( n \) is not prime, then \( n \) fails the SPSP test for at least \( \frac{3n}{4} \) values of \( a \) (mod \( n \)).

(I.e. a random choice of \( a \) will show \( n \) is composite \( \frac{3}{4} \) of the time.)

---

**Miller-Rabin SPSP Test**

- Given \( n-1 = 2^k d \) with odd \( d \), compute
  - \( a^2, a^d, a^{2d}, \ldots, a^{2^{k-1}d} \pmod{n} \)

If \( b_{2^j} \equiv 1 \pmod{n} \) or \( b_{2^j} \equiv -1 \pmod{n} \), then \( n \) is a prime.

**P**

How about finding factors of a composite number?
Finding factors:
Pollard rho method

If we know that \( n \) is composite (e.g., via Miller-Rabin or FLT), how do you factor it?

If \( n = pq \) (\( p < q \), say), then the basic idea is that

If \( u_1, u_2, \ldots, u_k \) are chosen at random, they are more likely to be distinct, mod \( n \), than they are mod \( p \). I.e., it is far more likely that for some \( i \) \( \text{gcd}(u_i - u_j, n) = \frac{n}{p} \)

\( (u_i - u_j, n) \) is a factor of \( n \).

The question is, how big should we expect \( k \) to be?

The prob that \( 1, u_1, \ldots, u_k \geq p \) are all distinct is

\[
(1 - \frac{1}{p}) (1 - \frac{2}{p}) \cdots (1 - \frac{k-1}{p}) \propto \exp \left( \frac{k^2}{2p} \right)
\]

It typically needs to check \( 2^{2n} \) or so for a good chance.

But need to compare \( \binom{k}{2} = \frac{(k-1)k}{2} \) things, \( \propto n^{3/4} \) calculations.
To make this into a practical method, we need to generate the \( u_i \) "pseudorandomly."

Typically, choose \( u_{i+1} = f(u_i) \pmod{n} \) where
\[
f = \text{poly, e.g. } f(x) = x^2 + b.
\]

This has the advantage that if
\[
u_i \equiv u_j \pmod{p} \text{ then } f(u_i) = u_{i+1} \equiv u_{j+1} = f(u_j)
\]

so the first time \( u_0 \equiv u_j \pmod{p} \) with \( i \neq j \geq 0 \)

further pairs
\[
\begin{array}{c}
\vdash u_i \equiv u_{i+r} \quad \text{all } i \geq r_0 \\
\vdash u_{i+r} \equiv u_{i+kr}
\end{array}
\]

so the first time \( kr \geq r_0 \), we have \( u_{kr} \equiv u_{kr} \pmod{p} \) all \( k \geq 1 \).

So, e.g.
\[
\begin{array}{c}
\vdash u_{kr} \equiv u_{2kr}
\end{array}
\]

So the Pollard \( p \)-test is usually set up as
\[
u_0 = \text{whatever} \quad \text{and } u_{i+1} = u_i^2 + b \pmod{n}
\]

then test \( \gcd(u_{kr} - u_m, n) \) if it is \( \geq 1 \) and \( u_m \),

we have found a factor.
fractions and repeating decimal representations.

\[
\frac{1}{3} = .3333\ldots \quad \frac{1}{7} = .142857142857\ldots = \overline{.142857}
\]

\[
\frac{1}{11} = .090909 \quad \frac{1}{12} = .166666\ldots = \overline{.16}
\]

every fraction has an (eventually) repeating decimal expansion.

Why? FLT!

Ex. \[
\frac{1}{13} = \frac{0.76923076923}{10^6} = 0.76923
\]

\[
= \frac{76923}{10^6} \cdot \left(1 + \frac{1}{10^6} + \frac{1}{10^{12}} + \ldots\right)
\]

\[
= \frac{76923}{10^6} \cdot \frac{1}{1 - \frac{1}{10^6}} = \frac{76923}{10^6} \cdot \frac{10^6}{10^6 - 1} = \frac{76923}{10^6 - 1}
\]

\[\text{I.e.} \quad 10^6 - 1 = 76923 \cdot 13\]

\[\text{I.e.} \quad \frac{10^6 - 1}{13} = 76923\]

More generally, \[
\frac{1}{n} = \text{blah} \quad \frac{1}{n} = \overline{\text{blah}}
\]

\[\text{if } 10^k - 1 = (\text{blah}) \cdot n \]

\[\iff \quad 10^k \equiv 1 \pmod{n}\]
But what if have \( 10^k \equiv 1 \) some \( k \)? \( \phi(n) = 1 \) !

I.e. \( (2, n) = (5, n) = 1 \). And what will \( \ell \) be?

\( \phi(n)! \) well, something dividing \( \phi(n) \).

\[
10^k \equiv 1 \pmod{n} \quad \text{then} \quad \ell = \left( k \phi(n) \right) / \phi(n) \quad \text{so}
\]

\[
10^{\frac{k}{n}} \equiv \left( 10^k \right)^{\frac{1}{n}} \equiv 1 \pmod{n} \quad \text{is smallest \( n \) divides \( \phi(n) \)}
\]

\( \square \cdot (2^n) = (5^n) = 1 \), then \( \frac{1}{n} \). (blah) where

\[
\text{length of (blah) = period } | \phi(n).
\]

Which \( n \) have the most possible period \( = \phi(n) \)?

\[
\text{Need } (10, n) = 1 \quad \text{and} \quad 10^{\phi(n)/n} \neq 1 \quad \text{for } 1 < k \mid \phi(n).
\]

\[
\text{What about when } (10, n) > 1? \quad n = 2^k 5^k \quad (p, n) = 1
\]

Then \( \frac{1}{n} = \frac{1}{(2^k 5^k p)} = \frac{a}{(2^k 5^k)} + \frac{b}{p} = \frac{pa + (2^k 5^k) b}{(2^k 5^k) p}
\]

\[
= \frac{a 2^k}{(10^k)} + \frac{b}{p}
\]

\( \leadsto \) so after some initial muddles, same period as \( \frac{1}{p} \).

1801: Gauss conjectured that there are only may primes \( p \) with period \( p - 1 \). Still open!