~~Def~~ How do you determine if a number n is prime?

Check if ~~every~~ any $x<n$ has $x|n$ ~~Too just~~

Check if any $x \le \sqrt{n}$ has $x|n$

If $(a,n)=1$ and $a^{n-1} \not\equiv 1 \pmod{n}$ then n <u>isn't</u> prime.

[Not perfect: $n = \cancel{\ldots}\ 561 = \cancel{\ldots}\ 3 \cdot 11 \cdot 17$ Carmichael #s

$2|560$, $10|560$, ~~$18|560$~~ $16|560$

$560 = 16 \cdot 35$

So $a^{560} \equiv_3 1$ $a^{560} \equiv_{11} 1$ $a^{560} \equiv_{17} 1$ $3,11,17 \mid a^{560}-1$

$\Rightarrow 3 \cdot 11 \cdot 17 \mid a^{560}-1$.]

A composite n for which $a^{n-1} \equiv_n 1$ is a <u>pseudoprime</u> to the base a

Wilson's Thm p is prime $\iff (p-1)! \equiv_p 1$.

Computationally onerous

If p is prime, then $x^2 \equiv_p 1 \Rightarrow x \equiv_p \pm 1$.

If n is odd, write $n-1 = 2^k d$ with d odd

Then if n is prime $a^{n-1} \equiv_n 1$

$a^{2^k d} \equiv_n 1$; look at $a^d, a^{2d}, a^{2^2 d}, \ldots a^{2^k d} \pmod{n}$

If n is prime The <u>last</u> one which isn't 1 <u>must</u> be -1.

So: If $n-1 = 2^k d$ and $a^{2^j d} \equiv_n 1$, $a^{2^{j-1} d} \not\equiv_n \pm 1$ then n is composite.

$n-1 = 2^k d$

but n is composite

If $a^{2^j d} \not\equiv_n 1$, $a^{2^{j+1} d} \equiv_n -1$ for some $j \le k$, then n is a <u>strong</u> pseudoprime to the base a. We

"n is spsp(a)"

$$\boxed{\text{Fact: if } n \text{ is not prime, then } n \text{ fails the spsp test for at least } \tfrac{3n}{4} \text{ values of } a \pmod n}$$

(Ie. a random choice of a will show n is composite ~~for~~ at least $3/4$ ths of the time.)

Miller-Rabin ~~SPS~~ ~~SPSP~~ Test $\quad n-1 = 2^k d$ $\quad d$ odd $\quad$ compute

$$\underset{\overset{\shortparallel}{b_0}}{a^d}, a^{2d}, a^{2^2 d}, \dots a^{2^k d} \pmod n$$

If ~~$b_k = 1$~~ $b_0 = 1$ or $b_i = -1$, $b_{i+1} = 1$ $\quad i<k$ then n is a probable prime

~~Pf~~

How about <u>finding</u> 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 ~~$u_1, \ldots, u_k$~~ $1 \le u_1, \ldots, u_k \le n$ 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,j

$$p \mid u_i - u_j \text{ but } n \nmid u_i - u_j, \text{ i.e. } p \le (u_i - u_j, n) < n$$

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

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

The prob that $1 \le u_1, \ldots, u_k \le p$ are all distinct is

$$\left(1 - \frac{1}{p}\right)\left(1 - \frac{2}{p}\right) \cdots \left(1 - \frac{k-1}{p}\right) \approx \exp\left(\frac{k^2}{2p}\right)$$

So typically need to ~~check~~ ~~$\sqrt{p}$~~ have $k \gtrapprox \sqrt{p}$ or so for a good chance.

But need to compare $\binom{k}{2} = \frac{(k-1)k}{2}$ things!

$\sim \approx n^{3/4}$ 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 $f =$ poly, e.g. $f(x) = x^2+b$.

this has the advantage that if

$$u_i \underset{p}{\equiv} u_j \text{ then } f(u_i) = u_{i+1} \underset{p}{\equiv} u_{j+1} = f(u_j)$$

So the first time $u_{i_0} \underset{p}{\equiv} u_{j_0}$ with ~~$k>j$~~ $i_0 - j_0 = r > 0$ we have all further pairs

$$\boxed{u_i \underset{p}{\equiv} u_{i+r} \quad \text{all } i \geq i_0}$$
$$\underset{p}{\equiv} u_{i+kr}$$

So the first time $kr \geq i_0$ we have $u_{kr} \underset{p}{\equiv} u_{lr}$ all $k \geq k_0$

So, e.g. $u_{k_0 r} \underset{p}{\equiv} u_{2k_0 r}$

~~Ex~~ So the Pollard ρ-test is usually set up as

$u_0 =$ whatever ~~the~~ $u_{i+1} = u_i^2 + b \pmod n$

then test $\gcd(u_{2i} - u_i, n)$ if it is >1 and $<n$, we have found a factor.

fractions and repeating decimal representations.

$\frac{1}{3} = .3333\ldots \qquad \frac{1}{7} = .142857142857\ldots = .\overline{142857}$

$\frac{1}{11} = .090909 \qquad \frac{1}{12} = .166666\ldots = .1\overline{6}$

<u>every</u> fraction has an ~~rep~~ (eventually) repeating decimal expansion

Why? FLT!

Ex $\frac{1}{13} = .\overline{076923}\,076923 = .\overline{076923}$

$$= \frac{76923}{10^6} + \frac{76923}{10^{12}} + \frac{76923}{10^{18}}$$

$$= \frac{76923}{10^6} \cdot \left(1 + \frac{1}{10^6} + \frac{1}{(10^6)^2} + \ldots\right)$$

$$= \frac{76923}{10^6} \cdot \frac{1}{1 - \frac{1}{10^6}} = \frac{76923}{10^6}\,\frac{10^6}{10^6 - 1} = \frac{76923}{10^6 - 1}$$

I.e. $\boxed{10^6 - 1 = 76923 \cdot 13}$

I.e., $10^6 \underset{13}{\equiv} 1$.

More generally, $\frac{1}{n} = .\text{blah blah blah}\ldots = .\overline{\text{blah}}$

$\Leftrightarrow$ (blah has k digits) $10^k - 1 = (\text{blah}) \cdot n$

$\Longleftrightarrow 10^k \underset{n}{\equiv} 1$.

But what #s have $10^k \underset{n}{\equiv} 1$ some k? $(10,n)=1$!

Ie. $(2,n)=(5,n)=1$. And what will k be?

$\phi(n)$! well, something <u>dividing</u> $\phi(n)$.

$10^k \underset{n}{\equiv} 1$ $\quad r=(k,\phi(n))$ then $r=kx+\phi(n)y$ so

$10^{r} \underset{n}{\equiv} (10^k)^x (10^{\phi(n)})^y \underset{n}{\equiv} 1^x \cdot 1^y = 1$ so <u>smallest</u> r divides $\phi(n)$

So if $(2,n)=(5,n)=1$, then $\frac{1}{n} = .\overline{(\text{blah})}$ where

length of (blah) = period $\mid \phi(n)$.

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

Need $(10,n)=1$ and $10^{\phi(n)/k} \underset{n}{\not\equiv} 1$ for $1<k \mid \phi(n)$

What about when $(10,n)>1$? $\quad n=2^m5^kp \quad (p,10)=1$

Then $\frac{1}{n} = \frac{1}{(2^m5^k)p} = \frac{a}{(2^m5^k)} + \frac{b}{p} = \frac{pa+(2^m5^k)b}{(2^m5^k)p}$

$= \frac{a5^m2^k}{(10)^{m+k}} + \frac{b}{p}$

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

1801: Gauss conjectured that there are ∞-ly many ~~primes~~ primes p with period $p-1$. Still open!

$10^{p-1} \not\equiv 1$ $\quad 10^{\frac{p-1}{k}} \not\equiv 1 \;\; \forall\, k \mid p-1$.