11/10

Fermat's little theorem.

If p is prime and $p \nmid a$ then $a^{p-1} \equiv 1 \bmod p$.

So if $a^{p-1} \not\equiv 1 \bmod p$ then p is composite. ~~EA~~ (converse is not true). If $a^{p-1} \equiv 1 \bmod p$ and p is not prime we call p a pseudoprime to the base a.

Factorization: We can try trial division. divide by 2, 3, ... $\sqrt{n}$.

Calculating ~~an~~ . Calculate $a^k \pmod n$.
and finding gcd

Raising #'s to powers Given integers a, k, n calculate $a^k \pmod n$

Very foolish method: Find a^k and reduce it mod n.

Less foolish: Find a^2, reduce mod n. Find $a^3 = a^2(a)$, and reduce mod n. This will take $k-1$ operations.

Good method: Successive squaring.

Find $A_0 = a$, $A_1 = A_0^2 \bmod n$ $A_2 = A_1^2 \bmod n$. ...
.... $A_r = A_{r-1}^2 \bmod n$ where $r = \lceil \log_2 k \rceil$

$k = k_0 + 2k_1 + 2^2 k_2 + \dots + 2^r k_r$ $k_i = 0, 1$, $k_r = 1$.

$a^k \pmod n$ is $\prod_{i, k_i = 1} A_i \bmod n$

Therefore we can find $a^k \pmod n$ in $\le 2 \log_2 k$ operations.

Greatest Common divisors of $a, b \in \mathbb{Z}$.

Method 1: factor a, b into primes and compare factorizations.

Method 2: Euclidean algorithm.

we can write $a = bq_1 + r_2$ where $q, r \in \mathbb{Z}$ $0 \le r < b$.

repeat: $b = r_2 q_2 + r_3$ $\quad 0 \le r_3 < r_2$

$$r_2 = r_3 q_3 + r_4$$

$$\vdots$$

$$r_n = \underline{\underline{r_{n+1}}}\, q_{n+1} + 0.$$

Claim: In the Euc. Alg. we have $r_{i+1} \le \frac{1}{2} r_{i-1}$.

If $r_i < \frac{1}{2} r_{i-1}$ then we're done. Otherwise, $r_i \ge \frac{1}{2} r_{i-1}$

$r_{i+1} = r_{i-1} - r_i q_i \le r_{i-1}\left(1 - \frac{1}{2} q_i\right)$

(and $q_i \ne 0$ because then $r_{i+1} = r_{i-1}$.)

so $q_i \ge 1$ and then $r_{i+1} \le (r_{i-1})(\frac{1}{2})$

So set $a \ge b$. Then $r_2 < b$, and repeatedly applying $(*)$

$r_{2i} < \frac{1}{2^{i-1}} b$ when $2^{i-1} > b$, then $r_{2i} < 1$, so $r_{2i} = 0$.

Prop. The Euclidean alg. computes $\gcd(a,b)$ in at most $2 \log_2 \{2a, 2b\}$ operations.

Factorization: Pollard's algorithm.

Let n be an integer. Say n has a prime factor p s.t. $p-1$ is a product of small primes to small powers.

Take $K = 2^{e_2} 3^{e_3} 5^{e_5} \cdots r^{e_r}$ (small exponents)

and compute $\gcd(a^k - 1, n)$ takes time $\sim \log kn$.

a any integer.

If p is a prime factor of n, and $p-1 \mid k$. Then by FLT $a^{p-1} \equiv 1$ modulo p.

$\Rightarrow a^k \equiv 1 \mod p$.

Recall that $p \mid a^k - 1$. So $\gcd(a^k-1, n) \geq p$. and p is a prime factor of n.

If $\gcd(a^k-1, n) \neq n$, then we have some factor of n.

If $\gcd(a^k-1, n) = n$, try different a.

If $\gcd(a^k-1, n) = 1$, then try a larger k.

Algorithm. Let $n \geq 2$

Step 1. Let $k = LCM(1, 2, 3, \dots, K)$ for some K.

Step 2. Choose a s.t. $1 < a < n$.

Step 3. Find $\gcd(a, n)$. If $\gcd(a,n) > 1$ Then have a factor. Otherwise go on to Step 4.

Step 4. Find $D = \gcd(a^k - 1, n)$. If $1 < D < n$, then D is a nontrivial factor of n.

if $D = 1$ choose larger k in step 1.

if $D = n$, change a in step 2.

Example. $n = 246082373$

try $a = 2$ $\quad k = 2^2 3^2 5 = 180$

$2^{180} \equiv 121299227 \pmod{n}$

And $\gcd(2^{180} - 1, n) = 1$.

So $\nexists$ p a prime factor of n with $p-1 \mid 180$.

Try $k = 2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$

Then $2^{2520} \equiv 101220672 \mod n$.

$\gcd(2^{2520}-1, n) = 2521$.

Dividing we get $n = 2521 \cdot 97613$