Modular arithmetic

For integer x,

$$x \bmod 2 = \text{least significant bit of } x = \begin{cases} 1 & \text{if } x \text{ is odd} \\ 0 & \text{if } x \text{ is even} \end{cases}$$

for integer $N \geq 1$,

$x \bmod N$ = remainder when divide x by N

$= r$ where $x = qN + r$ for integers q, r.

For example, mod 3 has 3 equivalence classes:

$$\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots$$
$$\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots$$
$$\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots$$

Basic fact: if $x \equiv x' \bmod N$ & $y \equiv y' \bmod N$,

then $x + y \equiv x' + y' \bmod N$

& $xy \equiv x'y' \bmod N$

Example: what's $2^{345} \bmod 31$? hint: $345 = 5 \times 69$

$$2^{345} \equiv (2^5)^{69} \equiv (32)^{69} \equiv 1 \bmod 31$$

~~Ex~~ e

For n-bit x, y, N

To compute $x+y \bmod N$:

- add $x+y$ then if $x+y \geq N$ output $(x+y-N)$ else output $(x+y)$

$\Rightarrow O(n)$ time.

To compute $xy \bmod N$:

- Compute xy ($O(n^2)$ bits long)
- Compute xy divided by N & output remainder

$\Rightarrow O(n^2)$ time.

To compute $x^y \bmod N$?

Easy idea: compute $x \bmod N$, $x^2 \bmod N$, $x^3 \bmod N$, $\vdots$, $x^y \bmod N$ } $\approx y$ rounds & $y \approx 2^n$

So exponential time.

Better: Powers of 2.

Example: $y = 25 = (11001)_2$

then $x^{25} \equiv x^{16} x^8 x \mod N$

So compute $\underbrace{x \bmod N,\ x^2 \bmod N,\ x^4 \bmod N,\ \ldots,\ x^{2^n} \bmod N}_{n \text{ rounds}}$

Repeated squaring:

for even y, $x^y = \left(x^{y/2}\right)^2$

for odd y, $x^y = (x)\left(x^{\lfloor y/2 \rfloor}\right)^2$

$\Rightarrow n$ rounds, $O(n^2)$ time/round so $\leq O(n^3)$ time.

Inverses (Multiplicative inverses):

For real numbers $a \times \frac{1}{a} = 1$

Now what's $\frac{1}{a} \mod N$?

Definition: z is the multiplicative inverse of $a \mod N$ if $az \equiv 1 \mod N$.

Can be at most one such z

Denote as $z \equiv a^{-1} \mod N$.

Example: $N=14$

$1^{-1} \equiv 1 \bmod 14$

$3^{-1} \equiv 5 \bmod 14$ $\quad 5^{-1} \equiv 3 \bmod 14$

$9^{-1} \equiv 11 \bmod 14$ $\quad 11^{-1} \equiv 9 \bmod 14$

$13^{-1} \equiv 13 \bmod 14$

$2^{-1}, 4^{-1}, 6^{-1}, 7^{-1}, 8^{-1}, 10^{-1}, 12^{-1} \bmod 14$ does not exist.

→ When does the inverse exist?

Theorem: $a^{-1} \bmod N$ exists iff $\underbrace{\gcd(a,N)=1}$,
a & N are relatively prime.

How to get it?

Use the Extended-Euclid algorithm.

Euclid's rule: for integers x, y where $x \geq y > 0$,

$\gcd(x,y) = \gcd(x \bmod y, y)$.

$\gcd(x,y) = \gcd(x-y, y)$

Euclid(x,y):

input: integers x, y where $x \geq y \geq 0$

output: $\gcd(x,y)$

if $y=0$, return(x)

else return (Euclid$(y, x \bmod y)$)

Observation: if $x \geq y$ then $x \bmod y < x/2$

Why? if $y \leq \frac{x}{2}$ then $x \bmod y < y \leq x/2$.

if $y > \frac{x}{2}$ then $x \bmod y = x - y < \frac{x}{2}$.

Thus, Euclid's alg. has $\leq 2n$ rounds & $O(n^2)$ time/round
$\Rightarrow O(n^3)$ total time.

Extended-Euclid(x, y):

input: integers x, y where $x \geq y \geq 0$
output: integers d, α, β where $d = \gcd(x, y)$ & $x\alpha + y\beta = d$

if $y = 0$, return $(x, 1, 0)$ Typo: ~~$(x, 0, 1)$~~

~~(d, α, β)~~ $(d, \alpha', \beta') =$ Extended-Euclid$(y, x \bmod y)$

return $(d, \beta', \alpha' - \lfloor \frac{x}{y} \rfloor \beta')$

Why do we care?

if $d = 1 = \gcd(x, y)$ then $1 \equiv x\alpha + y\beta$

So $1 \equiv x\alpha \bmod y$

$\alpha \equiv x^{-1} \bmod y$

gives a way to get $x^{-1} \bmod N$ when $\gcd(x, N) = 1$

Fermat's little theorem:

if p is prime then for all $a \not\equiv 0 \bmod p$,

$$a^{p-1} \equiv 1 \bmod p$$

$\Rightarrow$ Will use for testing if a given number $\mathbb{Z}$ is prime & for RSA cryptosystem.

Proof:

Let $S = \{1, 2, 3, \ldots, p-1\}$

Look at $S' = aS \bmod p = \{a \bmod p, 2a \bmod p, \ldots, (p-1)a \bmod p\}$

Example: $p = 7, a = 3$

$S = \{1, 2, 3, 4, 5, 6\}$, $S' = \{3, 6, 2, 5, 1, 4\}$

Claim: $S = S'$

Proof: elements of S' are distinct:

Suppose for $i \neq j$, $ai \equiv aj \bmod p$

since p is prime, $\gcd(a, p) = 1$ so $a^{-1} \bmod p$ exists.

$$aia^{-1} \equiv aja^{-1} \bmod p$$

$$i \equiv j \bmod p \quad \not\equiv$$

Similarly, if $ai \equiv 0 \bmod p$ then $i \equiv 0 \bmod p$.

So S' has $p-1$ non-zero elements. ∎

Since $S \equiv S' \bmod p$ (just different order)

$$\prod_{z \in S} z \equiv \prod_{z \in S'} z' \bmod p$$

$$(1)(2)(3)\cdots(p-1) \equiv (a)(2a)(3a)\cdots((p-1)a) \bmod p$$

$$1 \equiv a^{p-1} \bmod p$$

since p is prime, $i^{-1} \bmod p$ exists for $1 \le i \le p-1$. ∎

Euler's theorem: for any N, a, if $\gcd(a,N)=1$

then $a^{\phi(N)} \equiv 1 \bmod N$,

where $\phi(N) = \#$ integers $b \in \{1,2,\ldots,N\}$

where $\gcd(b,N)=1$

For $N=p$ where p is prime then $\phi(p)=p-1$

So this gives Fermat's little theorem.

For primes p, q let $N=pq$.

Then $\phi(N)=(p-1)(q-1)$

so for a rel. prime to N, $a^{(p-1)(q-1)} \equiv 1 \bmod N$.

Back to Fermat's little theorem:

Take b, c where $bc \equiv 1 \mod (p-1)$

So $b \equiv c^{-1} \mod (p-1)$

thus, $bc = 1 + k(p-1)$ for integer k.

Therefore, $a^{bc} \equiv (a)(a^{p-1})^{k} \equiv a \mod p$ by

Looking at Euler's theorem:

For primes p, q, let $N = pq$.

Take d, e where $de \equiv 1 \mod (p-1)(q-1)$.

So $de = 1 + k(p-1)(q-1)$

for a rel. prime to N,

$$a^{de} \equiv (a)\left(a^{(p-1)(q-1)}\right)^{N} \equiv a \mod N.$$