Date
Page

Number Theory

Division Theorem

Divide a by $b > 0$

$$a = qb + r$$

$$0 \leq r \leq b - 1$$

Congruence:

a is said to be congruent to b modulo m iff a and b leave same remainder when divided by m

we denote $a \equiv_m b$

or $a \equiv b \bmod m$

eg $11 \equiv_8 3 \equiv_8 27$

Results on congruent arithmetic

1. If $a \equiv b \bmod m$ and $c \equiv d \bmod m$ then $a + c \equiv b + d \bmod m$

2. If . . . .
then $ac \equiv b.d \bmod m$

3. $(a+b) \bmod m \equiv (a \bmod m + b \bmod m) \bmod m$

4. $ab \bmod m \equiv ((a \bmod m)(b \bmod m)) \bmod m$

5. $a^n \bmod m \equiv (\overbrace{a \bmod m}^{b})^n \bmod m$
$\equiv ((b.b) \bmod m . b \bmod m) \bmod m$

Square and multiply algorithm

M-3 $3^{17} \bmod 5$

$3^2 \bmod 5 = 4$

$3^3 \bmod 5 = 4 \cdot 3 \bmod 5 = 2$

$3^4 \bmod 5 = 2 \cdot 3 \bmod 5 \equiv$

$\vdots$

$3^{17} \equiv \ldots$

M-4 $3 \bmod 5 \equiv y$

$3^2 \bmod 5 \equiv y^2 \equiv z$

$3^4 \bmod 5 \equiv z^2 \equiv u$

$3^8 \bmod 5 \equiv u^2 \equiv v$

$3^{16} \bmod 5 \equiv v^2$

Multiply 3^{16} with 3

$x \bmod n$

Convert it into binary

$x = 1$

$p = 1$

GCD

Factorization

Euclid's algorithm

$a > b$

$a = bq_1 + r_1$

$b = r_1 q_2 + r_2$

$r_1 = r_2 q_3 + r_3$

$r_{n-2} = r_{n-1} q_n + r_n$

$r_{n-1} = r_n q_{n+1} + 0$

Bezout's Theorem

If integers x and y

s.t. $\gcd(a, b) = ax + by$