ECE 471/571. Modular Arithmetic & early ciphers

$GCD(a,b) = \max[k,\ s.t\ k|a,\ k|b]$

$GCD(60, 24) = 12$

1, 2, 3, 4, 6, 12

. . . . . 6, 12, 15, 20, 30

if a, b are relatively prime,

$\Leftrightarrow GCD(a,b) = 1$

$GCD(8, 15) = 1$

$\underline{1}$, 2, 4, 8. $\underline{1}$, 3, 5, 15

Euclidean Alg. $a \geq b \geq 0$

then $GCD(a, b) = GCD(b, a \bmod b)$

$GCD(55, \underline{22}) = GCD(22, 11)$

$= GCD(11, 0)$

$= \underline{11}$

$GCD(18, 12) = GCD(12, 6) = 6$

$GDD(11, 10) = GCD(10, 1) = 1$

e.g. $a = 710$, $b = 310$.

① $\overset{a}{710} = \overset{q_1}{2} \times \overset{b}{310} + \overset{r_1}{90}$

② $310 = \overset{q_2}{3} \times 90 + \overset{r_2}{40}$

③ $90 = \overset{q_3}{2} \times 40 + \overset{r_3}{10}$

④ $40 = 4 \times 10 + 0$

$gcd(10, 0) = 10 = gcd(710, 310)$.

$gcd(a,b) = gcd(|a|, |b|)$.

$gcd(a, 0) = |a|$

Extended Euclidean Alg.

given a, b integers

exists x, y. int. s.t.

$gcd(a,b) = d = ax + by$.

if a, b are rel. prime.

$$\gcd(a,b)=1 = ax+by.$$

multiplicative inverse of b mod a

$$1 = (\underline{ax} + by) \bmod a = b \cdot y \bmod a$$

$$y = b^{-1} \bmod a.$$

e.g $\boxed{\begin{matrix} a = 42 \\ b = 30 \end{matrix}}$

$$x_i = x_{i-2} - q_i \cdot x_{i-1}$$

$$y_i = y_{i-2} - q_i \cdot y_{i-1}$$

a: $x_{-1} = 1$ $y_{-1} = 0$

b: $x_0 = 0$ $y_0 = 1$

$$a = \overset{x_{-1}}{1} \cdot a + \overset{y_{-1}}{0} \cdot b$$

$$b = \underset{x_0}{0} \cdot a + \underset{y_0}{1} \cdot b$$

i	r_i	q_i	x_i	y_i
-1	$a=42$	·	1	0
0	$b=30$	·	0	1
1	12	1	1	-1
2	6	2	-2	3

3	0	2	✗	✗

$$6 = -2 \cdot 42 + 3 \cdot 30 \quad \checkmark$$

---

prime numbers

1, 2, 3, 5. 7, 11, 13, 17

int. $a > 1$.

$$91 = 7 \times 13.$$

$$60 = 2^2 \times 3^1 \times 5^1 = 4 \times 15$$

$$11011 = 7 \times 11^2 \times 13$$

$$a = p_1^{a_1} \times p_2^{a_2} \cdots \times p_n^{a_n}$$

$$p_1 < p_2 < \cdots < p_n$$

are prime #s

$a_i > 0$

fundamental theorem of arithmetic