LEC 8 09/13/99

DIVISION OF INTEGERS

Th $\forall a, d \in \mathbb{Z}\ \ d>0\ \ \exists! q, r$

$a = dq + r \qquad 0 \le r < d$

PROOF. ASSUME $a>0$, FOR SIMPLISITY
SINCE $a \le a \cdot d$ THERE EXISTS THE FIRST $q \le a$ SUCH THAT $q \cdot d \le a < (q+1) \cdot d$
LET $r := a - qd$. THEN $a = q \cdot d + r$, $r < d$

UNIQUENESS: SUPPOSE $a = dq_1 + r_1 = dq_2 + r_2$
$0 = d(q_1 - q_2) + (r_1 - r_2)$
$(q_2 - q_1)d = r_1 - r_2$, BUT $|(q_2 - q_1)d| = |q_2 - q_1| \cdot d \ge d$, IF $q_2 \ne q_1$
$|r_1 - r_2| < d$.
THEREFORE $q_2 = q_1$; $r_2 = r_1$

d - DIVISOR
a - DIVIDENT
q - QUOTIENT
r - REMAINDER

EXAMPLES: $a=17, d=3 \Rightarrow q=5, r=2$
$17 = 3 \cdot 5 + 2$
$a=-17, d=3 \Rightarrow q=-6, r=1$
$-17 = 3 \cdot (-6) + 1$

def. $a, b \in \mathbb{Z}$, $a \ne 0$. a DIVIDES b IF
$\exists c \in \mathbb{Z}\ \ b = a \cdot c$ $(a|b)$
(a: MULTIPLE OF a; c: FACTOR OF b)

EXAMPLES $3|12$ $17|17$ BUT NOT $-5|12$

$a|b \wedge a|c \Rightarrow a|(b+c)$
$a \cdot x = b \wedge a \cdot y = c \Rightarrow a(x+y) = ax + ay = b + c$
$a|b \Rightarrow a|bc$ $\qquad a|b \wedge b|c \Rightarrow a|c$
$ax = b \Rightarrow a(xc) = bc$ $\qquad ax = b \wedge by = c \Rightarrow axy = c$

def PRIME: $p>1$ SUCH THAT
$q|p \wedge q>0 \Rightarrow q=1 \vee q=p$
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, ...

COMPOSITE: $p>1$ AND p IS NOT A PRIME.

FUNDAMENTAL THEOREM OF ARITHMETIC:
ANY INTEGER >1 IS A UNIQUE PRODUCT OF PRIMES

$30 = 2 \cdot 3 \cdot 5$ $\qquad 99 = 3 \cdot 3 \cdot 11 = 3^2 \cdot 11$
$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$ $\qquad 101 = 101$

Th A COMPOSITE n HAS A PRIME DIVISOR $\le \sqrt{n}$

PROOF. n HAS A FACTOR a, $1 < a < n$
$n = a \cdot b \Rightarrow b > 1$. IF BOTH $a, b > \sqrt{n}$
THEN $a \cdot b > \sqrt{n} \cdot \sqrt{n} = n$. THEREFORE $a \le \sqrt{n} \vee b \le \sqrt{n}$
SUPPOSE $a \le \sqrt{n}$. ANY PRIME DIVISOR p OF a:
$p|a \wedge a|n \Rightarrow p|n$
$p \le a \le \sqrt{n} \Rightarrow p \le \sqrt{n}$

COROLLARY: 101 IS A PRIME, SINCE $\sqrt{101} < 11$
AND $2, 3, 5, 7 \nmid 101$

GREATEST COMMON DIVISOR OF $a, b \ne 0$
THE LARGEST d SUCH THAT $d|a \wedge d|b$.
$\gcd(a,b)$ (OR JUST (a,b))

EXAMPLES: $\gcd(36, 48) = 12$; $\gcd(11, 20) = 1$

a, b ARE RELATIVELY PRIME IF $\gcd(a,b) = 1$

LEAST COMMON MULTIPLE OF $a, b > 0$
THE SMALLEST POSITIVE INTEGER ℓ SUCH THAT
$a|\ell \wedge b|\ell$ $\qquad \operatorname{lcm}(a,b)$

EXAMPLES: $\operatorname{lcm}(12, 15) = 60$
$\operatorname{lcm}(2^3 \cdot 3 \cdot 7^2,\ 2 \cdot 3^2 \cdot 5 \cdot 7) =$
$= 2^{\max(3,1)} \cdot 3^{\max(1,2)} \cdot 5^{\max(0,1)} \cdot 7^{\max(2,1)} =$
$= 2^3 \cdot 3^2 \cdot 5 \cdot 7^2 = 17640$

Th $a \cdot b = \gcd(a,b) \cdot \operatorname{lcm}(a,b)$
EXERCISE!

$a \bmod m$ = REMAINDER WHEN a IS DIVIDED BY m $(m>0)$

$17 \bmod 3 = 2$; $-17 \bmod 3 = 1$

$a \equiv b \pmod m$ $\quad$ $a \bmod m = b \bmod m$ $\quad$ $m \mid (a-b)$

a IS CONGRUENT TO b modulo m.

$$\left.\begin{array}{l} a \equiv b \pmod m \\ c \equiv d \pmod m \end{array}\right\} \Rightarrow \begin{array}{l} a+c \equiv b+d \pmod m \\ a \cdot c \equiv b \cdot d \pmod m \end{array}$$

$10 \equiv -17 \pmod 3$; $5 \equiv 17 \pmod 3$

APPLICATIONS

HASHING FUNCTIONS: $h(k) = k \bmod m$ (KEY (e.g. SS#); HASHING FUNCTION; MEMORY LOCATION)

$h(123456789) = 123456789 \bmod 111 = 36$

PSEUDORANDOM NUMBERS: LINEAR CONGRUENTAL METHOD

$$x_{n+1} = (a x_n + c) \bmod m \; ; \quad x_0$$

a: MULTIPLIER; c: INCREMENT; m: MODULUS; x_0: SEED

$0 \le a < m$, $0 \le c < m$, $0 \le x_0 < m$

SEQUENCE $\{x_n\}$ OF PSEUDORANDOM NUMBERS

TOY EXAMPLE: $x_{n+1} = (7x_n + 4) \bmod 9$; $x_0 = 3$

$\{x_n\}$: 3, 7, 8, 6, 1, 2, 0, 4, 5, 3, 7, 8, 6, 1, 2, 0, 4, 5, 3

PERIOD

REAL LIFE EXAMPLE: $m = 2^{31}-1$, $a = 7^5 = 16807$

PERIOD IS $2^{31}-2$ LONG!

ENCRYPTIONS: MAKING A MESSAGE SECRET

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

CAESAR'S ENCRYPTION: $f(p) = (p+3) \bmod 26$

DECRIPTION: $f^{-1}(p) = (p-3) \bmod 26$

f^{-1}(PHHW BRX LQ WKH SDUN) = MEET YOU IN THE PARK

HW 2.3: 10e,f 28c,d 46b