3.4 Integers & Division

Defn ① If $a, b \in \mathbb{Z}$, $a \neq 0$, $\underline{a \text{ divides } b}$ if $\exists\ c \in \mathbb{Z} \Rightarrow b = ac$.

equivalently a is a factor of b

or b is a multiple of a

notation: $a \mid b$ (we use $a \nmid b$ when a does not divide b)

Thm 1 $a, b, c \in \mathbb{Z}$. (i) $a \mid b$ and $a \mid c \Rightarrow a \mid (b+c)$

(ii) $a \mid b \Rightarrow a \mid bc \quad \forall\ c \in \mathbb{Z}$.

(iii) $a \mid b$ and $b \mid c \Rightarrow a \mid c$.

Corollary: If $a, b, c \in \mathbb{Z} \Rightarrow a \mid b$ and $a \mid c$, then $a \mid (mb + nc)$ $\forall\ m, n \in \mathbb{Z}$.

Thm 2 Division Algorithm Let $a \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$. Then $\exists$ unique integers q & $r \Rightarrow 0 \leq r < d$ and $a = dq + r$.

q is called quotient, r is remainder

Defn ② For Division Algorithm, d = divisor, a = dividend

and $q = a \text{ div } d$ $\quad r = a \bmod d$

Ex 1 Evaluate if these statements are true or false.

(a) $17 \mid 84$

(b) $11 \mid 143$

(c) $30 \mid 5$

3.4 (cont)

Ex 2 Use Division Algorithm to find q & r.

remember
$0 \leq r < d$

(a) 44 divided by 8

(b) $777 \div 21$

(c) $-202 \div 87$

(d) $-1 \div 23$

3.4 (cont)

Ex 3 Show that if $a, b, c \in \mathbb{Z}$, $c \neq 0$, and $ac \mid bc$, then $a \mid b$.

Modular Arithmetic

Defn ③ If $a, b \in \mathbb{Z}$, $m \in \mathbb{Z}^+$, then a is congruent to b modulo m if $m \mid (a-b)$.

notation: $a \equiv b \pmod{m}$

($a \not\equiv b \pmod{m}$ means a is not congruent to b modulo m)

(colloquially we can say that a & b have same remainder when divided by m)

Thm 3 Let $a, b \in \mathbb{Z}$, $m \in \mathbb{Z}^+$. Then $a \equiv b \pmod{m}$ $\iff$ $a \bmod m = b \bmod m$

Thm 4 Let $m \in \mathbb{Z}^+$, $a, b \in \mathbb{Z}$.
$a \equiv b \pmod{m} \iff \exists\, k \in \mathbb{Z} \ni a = b + km$

★ note difference in bold between bold faced "mod" vs "mod"

3.4 (cont)

Corollary $m \in \mathbb{Z}^+$, $a, b \in \mathbb{Z}$. Then

(i) $(a+b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$

(ii) $ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$

Ex 4 Evaluate.

(a) $13 \bmod 3$

(b) $-97 \bmod 11$

(c) $155 \bmod 19$

Ex 5 List five integers that are congruent to $4 \pmod{12}$.

Ex 6 Encrypt the message "MATH IS FUN" by translating letters into numbers (1 thru 26), applying the encryption fn, & then translating back to letters.

MATH ^ IS ^ FUN ⇒ 13 1 20 8 ^ 9 19 ^ 6 21 14

$f(p) = (p + 11) \bmod 26$

3.5 Primes & Greatest Common Divisors

Defn ① $p \in \mathbb{Z}^+$ is **prime** if the only positive factors of p are 1 and p. If $p > 1$ and it's not prime, then it's composite.

Thm 1 Fundamental Thm of Arithmetic

Every positive integer p, $p > 1$, can be written uniquely as a prime or the product of 2 or more primes.

Thm 2 If n is composite, then n has a prime divisor less than or equal to $\sqrt{n}$.

Pf n composite $\Rightarrow \exists\, a \in \mathbb{Z}^+ \ni a$ is factor of n and $1 < a < n \Rightarrow n = ab$ for some $b \in \mathbb{Z}^+$, $b > 1$.

- If $a > \sqrt{n}$ and $b > \sqrt{n}$, then $ab > \sqrt{n}\sqrt{n} > n$ which is a contradiction.

$\Rightarrow$ either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$ · //

Ex 1 Show that 115 is prime.

3.5 (cont)

Ex 2 Find prime factorization for these numbers.

(a) 289 (b) 899

Thm 3 There are infinitely many primes.

Pf (By Contradiction) Assume there are finitely many prime #s, $p_1, p_2, \ldots, p_n$. Then let

$a = p_1 p_2 \cdots p_n + 1$. By Fundamental Thm of Arithmetic, a is either prime or composite. Notice that none of the prime #s $p_1, \ldots, p_n$ divide a. That means that a cannot be composite $\Rightarrow$ a is prime $\Rightarrow$ we have a contradiction. There must be at least one more prime than p_n. $\Rightarrow$ There are infinitely many primes. //

3.5 (cont)

Ex 3 We call a positive integer perfect if it equals the sum of its positive divisors other than itself.

Show that (a) 6 and (b) 28 are perfect.

Defn ② $a, b \in \mathbb{Z}$, $a^2 + b^2 \neq 0$. The largest integer d s.t. $d|a$ and $d|b$ is called greatest common divisor (or greatest common factor) of a and b.

notation: $\gcd(a,b)$ (or $\text{gcf}(a,b)$)

Defn ③ $a, b \in \mathbb{Z}$ are relatively prime if $\gcd(a,b) = 1$.

(i.e. they have no common factors other than 1)

Defn ④ Integers $a_1, a_2, \ldots, a_n$ are pairwise relatively prime if $\gcd(a_i, a_j) = 1 \quad \forall \ 1 \leq i < j \leq n$.

Defn ⑤ least common multiple of $a, b \in \mathbb{Z}^+$ is smallest positive integer that is divisible by both a & b.

notation: $\text{lcm}(a,b)$

3.5 (cont)

Thm 5 $a, b \in \mathbb{Z}^+$

$ab = \gcd(a,b)\,\text{lcm}(a,b)$

Ex 4 Which integers are pairwise relatively prime?

(a) 11, 15, 19

(b) 14, 15, 21

(c) 7, 8, 9, 11

Ex 5 Find gcd and lcm of these pairs of integers.

(a) $3^7 \cdot 5^3 \cdot 7^3$ and $2^{11} \cdot 3^5 \cdot 5^9$

3.5 (cont)

Ex 5 (cont)

(b) $41 \cdot 43 \cdot 53$ and $41 \cdot 43 \cdot 53$

(c) 0 and 1111

(d) 23^{31} and 23^{17}

Ex 6 Find the smallest positive integer w/ exactly 7 different factors.