MAT2440, Classwork39, Spring2025

ID:_____ Name:_____

1. Definition of Prime.

   Every integer greater than 1 is divisible by at least two positive integers, 1 and itself.

   If a positive integer $p > 1$ has exactly two positive factors, 1 and itself, then it is called prime. Otherwise, it is called composite and there exists an integer a such that $a \mid p$ and $1 < a < p$.

2. Primes < 50: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.

3. Show that 5 is a prime and 6 is a composite number.

   5: $1|5$ and $5|5$ no more factors $\Rightarrow$ 5 is a prime

   6: $1|6$, $2|6$, $3|6$, $6|6$ $\Rightarrow$ 6 is NOT a prime, 6 is composite

4. The Fundamental Theorem of Arithmetic.

Every integer > 1 can be written uniquely as a prime or as the products of primes.

This gives prime factorization of integers.

5. Find the prime factorizations of 100, 641, 999, and 1024.

   $100 = 2 \cdot 50 = 2 \cdot 2 \cdot 25 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$

   $641 = 1 \cdot 641$

   $999 = 9 \cdot 111 = 3^2 \cdot 3 \cdot 37 = 3^3 \cdot 37$

   $1024 = 2 \cdot 512 = 2 \cdot 2 \cdot 256 = 2 \cdot 2 \cdot 2 \cdot 128 = \cdots = 2^{10}$

6. Greatest Common Divisors.

   Let a, b be positive integers. The largest integer d such that $d \mid a$ and $d \mid b$ is called the greatest common divisor of a and b, denoted by $\gcd(a, b)$

7. What is gcd(24, 36)?

   24 has factors 1, 2, 3, 4, 6, 8, 12, 24

   36 has factors 1, 2, 3, 4, 6, 9, 12, 18, 36

   $\Rightarrow$ common factors 1, 2, 3, 4, 6, 12

   $\gcd(24, 36) = 12$

8. Relatively Prime.

If $\gcd(a_1, a_2, \cdots, a_n) = 1$, we say $a_1, a_2, \cdots, a_n$ are relatively prime.

For example, $\gcd(14, 27) =$ 1

14 has factors 1, 2, 7, 14

27 has factors 1, 3, 9, 27

9. Find GCD: **Use prime factorization.**

If $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ and $b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$, then we have

$$\gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)}.$$

10. Find gcd(24, 36) by using prime factorization.

$24 = 2^3 \times 3^1$

$36 = 2^2 \times 3^2$ $\Rightarrow \gcd(24, 36) = 2^2 \cdot 3^1$

$= 4 \cdot 3 = 12$

11. Find GCD: **The Euclidean Algorithm**.

For example, let $d = \gcd(24, 36)$. We have $d|24$ and $d|36$.

36 = 1 × **24** + 12, then 12 = 36 **mod** 24 and $d|12$. It implies $d = \gcd(24, 12)$.

gcd(24, 36 mod 24)

24 = 2 × **12** + 0, then 0 = 24 **mod** 12 and $d|0$. It implies $d = \gcd(12, 0)$.

gcd(24 mod 12, 12)

Thus, $d = 12$.

$\gcd(a, b) = \gcd(a \bmod b, b) = \gcd(a, b \bmod a)$

12. **The Euclidean Algorithm.**

Let $a = qb + r$, where a, b, q, r are integers. Then gcd(a, b) = gcd(b, r).

"replace the dividend by remainder"

13. Find gcd(91, 287) by using the Euclidean algorithm.

$\gcd(91, 287) = \gcd(91, 287 \bmod 91)$

$= \gcd(91, 14)$

$= \gcd(91 \bmod 14, 14)$

$= \gcd(7, 14)$

$= \gcd(7, 14 \bmod 7)$

$= \gcd(7, 0) = 7$

$91 \overline{)287}$ 3, 273, 14 ← remainder

$14 \overline{)91}$ 6, 84, 7 ← remainder

$7 \overline{)14}$ 2, 14, 0 ← remainder