

EXERCISE SET 1

DISCRETE MATHEMATICS

For the following list of problems, let $a, b, c, d \in \mathbb{Z}$ and $m \in \mathbb{N}_+$ be arbitrary, and let φ be Euler's totient function.

1. Warm-up

- (a) Show that $\gcd(a, b) \mid a$.
- (b) Show that $a \mid b$ implies either a is odd or b is even.
- (c) Show that if $c \neq 0$ then $(ac \mid bc) \Rightarrow (a \mid b)$.

2. Easy

- (a) Show that, if $3 \nmid a$, then $3 \mid (a+1)(a+2)$.
- (b) Show that $4 \nmid a^2 + 2$.
- (c) Show that $b \equiv c \pmod{\varphi(m)} \not\Rightarrow a^b \equiv a^c \pmod{m}$.
- (d) Is it the case that $((a \mid bc) \wedge a \neq 0) \Rightarrow ((a \mid b) \vee (a \mid c))$?

3. Medium

- (a) Show that $b \equiv c \pmod{m} \not\Rightarrow a^b \equiv a^c \pmod{m}$.
- (b) Show that if $\gcd(a, b) > 2$ then $(\forall n \in \mathbb{N})(n > 2 \Rightarrow n^2 \nmid \gcd(a, b))$.
- (c) Show that if $\gcd(a, b) > 2$ then $\gcd(a, b)$ is a product of *distinct* primes.
- (d) Show that if $a \neq 0$ and $b \neq 0$ then $a \equiv b \pmod{m} \Rightarrow \gcd(a, m) = \gcd(b, m)$.

4. Hard

- (a) Let p be prime. Show $a^p \equiv a \pmod{p}$.
- (b) Let $\text{lcm}(a, b)$ be the *least common multiple* of a and b . Show that $ab = \gcd(a, b) \text{lcm}(a, b)$.

1. Algorithm practice

- (a) Verify **by hand** that $\gcd(69, 51) = 3$ by computing $\gcd(69, 51)$.
- (b) Verify **by hand** that $\gcd(234, 44) = 2$ by computing $\gcd(234, 44)$.

2. Programming practice

- (a) Verify that $\gcd(69, 51) = 3$ and $3 = 2 \cdot 69 - 9 \cdot 15$ by computing $\text{egcd}(69, 51)$.
- (b) Verify that $\gcd(234, 44) = 2$ and $2 = -3 \cdot 234 + 16 \cdot 44$ by computing $\text{egcd}(234, 44)$.