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 $\big(ac \mid bc\big) \;\Rightarrow\; \big(a \mid b\big)$.
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 $\Big(\big(a \mid bc\big) \wedge a \neq 0\Big) \;\Rightarrow\; \Big(\big(a \mid b\big) \vee \big(a \mid c\big)\Big)$?
   (e) If $p \neq q$ are both prime, show that $\Big(\big(p \mid a\big) \wedge \big(q \mid a\big)\Big) \;\Rightarrow\; pq \mid a$.
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 $(\forall n \in \mathbb{N})\Big(n > 2 \;\Rightarrow\; n^2 \nmid \gcd(a, b)\Big)$.
   (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 $a^p \equiv p \pmod{p}$.
   (b) Let $\operatorname{lcm}(a, b)$ be the *least common multiple* of a and b. Show that $ab = \gcd(a, b)\operatorname{lcm}(a, b)$.

---

1. **Algorithm practice**
   (a) Verify **by hand** that $\gcd(69, 51) = 3$ by computing $\texttt{gcd}(69, 51)$.
   (b) Verify **by hand** that $\gcd(234, 44) = 2$ by computing $\texttt{gcd}(234, 44)$.
2. **Programming practice**
   (a) Verify that $\gcd(69, 51) = 3$ and $3 = 2 \cdot 69 - 9 \cdot 15$ by computing $\texttt{egcd}(69, 51)$.
   (b) Verify that $\gcd(234, 44) = 2$ and $2 = -3 \cdot 234 + 16 \cdot 44$ by computing $\texttt{egcd}(234, 44)$.