Problem Set 1
Arithmetic of Integers

Guidelines: Try to solve all the problems on your own. If you face any difficulty, discuss with the TA during the tutorial session.

1. Let p be a prime. If $p|(ab)$, show that $p|a$ or $p|b$. More generally, show that if $p|(a_1a_2\cdots a_n)$, then $p|a_i$ for some $i \in \{1, 2, \cdots, n\}$.

2. Let, $a, b \in \mathbb{N}$ with $d = \gcd(a, b) = ua + vb$ for some $u, v \in \mathbb{Z}$. Demonstrate that u, v are not unique. Now, assume that $(a, b) \neq (1, 1)$. Prove that:
   (a) If $d = 1$, then u, v can be chosen to satisfy $|u| \leq b$ and $|v| \leq a$.
   (b) In general, u, v can be chosen to satisfy $|u| \leq b/d$ and $|v| \leq a/d$.

3. Prove that for any $r \in \mathbb{N}$, the product of r consecutive integers is divisible by $r!$. (Please avoid the argument that binomial coefficient $\binom{n}{r}$ is an integer.)

4. Let p be a prime and $a, b \in \mathbb{Z}$. Prove the following assertions.
   (a) $\binom{p}{k} \equiv 0 \pmod{p}$ for all $k = 1, \cdots, p-1$, where $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ is the binomial coefficient.
   (b) If $a^p \equiv b^p \pmod{p}$, then $a^p \equiv b^p \pmod{p^2}$.

5. Let a, b, c be a non-zero integers, and $d = \gcd(a, b)$.
   (a) Prove that the equation $ax + by = c$ is solvable in *integer* values of x, y if and only if $d|c$.
   (b) Suppose that $d|c$, and (s, t) is one solution of the congruence of Part (a). Prove that all solutions of this congruence can be given as $(s + k(b/d), t - k(a/d))$ for all $k \in \mathbb{Z}$. Describe how one solution (s, t) can be efficiently computed.

6. Suppose that we want to compute $x^r y^s \pmod{m}$, where r and s are positive integers of the same bit size. By repeated square-and-multiply algorithm, one can compute $x^r \pmod{m}$ and $y^s \pmod{m}$ independently, and then multiply two values. Alternatively, one may rewrite the square-and-multiply algorithm using only one loop in which the bits of both the exponents r and s are simultaneously considered. After each square operation, one multiplies by 1, x, y or xy.
   (a) Elaborate the algorithm outlined above. What speedup is this modification expected to produce?
   (b) Generalize the concept to the computation of $x^r y^s z^t \pmod{m}$, and analyze the speedup.

7. Find the simultaneous solution of the congruences: $7x \equiv 8 \pmod 9$, $x \equiv 9 \pmod{10}$, and $2x \equiv 3 \pmod{11}$.

8. [*Generalized Chinese remainder theorem*] Let $m_1, m_2, \ldots, m_t$ be t moduli (not necessarily coprime to one another).
   (a) Prove that the congruences $x \equiv a_i \pmod{m_i}$ for $i = 1, 2, \ldots, t$ are simultaneously solvable if and only if $\gcd(m_i, m_j) | (a_i - a_j)$ for every pair (i, j) with $i \neq j$. Show also that in this case the solution is unique modulo $\operatorname{lcm}(m_1, m_2, \ldots, m_t)$.
   (b) Design an algorithm that, given moduli m_1, m_2 and integers a_1, a_2 with $\gcd(m_1, m_2) | (a_1 - a_2)$, computes a simultaneous solution of the congruences $x \equiv a_i \pmod{m_i}$ for $i = 1, 2$.
   (c) Design an algorithm to implement the generalized CRT on $t \geq 2$ moduli.

9. Let $n = pq$ with two distinct primes p, q. Devise a polynomial-time algorithm to compute p, q from the knowledge of n and $\phi(n)$.

10. Let p be a prime > 3. Prove that 3 is a quadratic residue modulo p if and only if $p \equiv \pm 1 \pmod{12}$.

11. Let p be an odd prime. Prove the congruence $x^2 \equiv -1 \pmod p$ is solvable if and only if $p \equiv 1 \pmod 4$.

12. Let p be a prime.
   (a) Prove that the congruence $x^2 \equiv -2 \pmod p$ is solvable if and only if $p = 2$ or $p \equiv 1$ or $3 \pmod 8$.
   (b) Show that p can be expressed as $a^2 + 2b^2$ with $a, b \in \mathbb{Z}$ if and only if $p = -2$ or $p \equiv 1 \pmod 8$ or $3 \pmod 8$.

13. Let p be an odd prime, $a \in \mathbb{Z}_p^*$, and $e \in \mathbb{N}$. Prove that the multiplicative order of $1 + ap$ modulo p^e is p^{e-1}. (**Remarks:** This result can be used to obtain primitive roots modulo p^e).

14. Let m be a modulus having a primitive root, and $a \in \mathbb{Z}_m^*$. Prove that a is a primitive root modulo m if and only if $a^{\phi(m)/q} \not\equiv 1 \pmod m$ for every prime divisor q of $\phi(m)$. Design an algorithm that, given $a \in \mathbb{Z}_m^*$ and the prime factorization of $\phi(m)$, determines whether a is a primitive root modulo m.