CS 70 Discrete Mathematics and Probability Theory
Fall 2013 Vazirani Modular Arithmetic Practice

1. **Modular arithmetic**

   Solve the following equations for x and y modulo the indicated modulus, or show that no solution exists. Show your work.

   (a) $7x \equiv 1 \pmod{15}$.

   (b) $10x + 20 \equiv 11 \pmod{23}$.

   (c) $5x + 15 \equiv 4 \pmod{20}$.

   (d) The system of simultaneous equations $3x + 2y \equiv 0 \pmod{7}$ and $2x + y \equiv 4 \pmod{7}$.

2. **Modular inverse**

   Prove that the equation $ax \equiv ay \bmod n$ implies $x \equiv y \bmod n$ whenever $\gcd(a,n) = 1$. Show that the condition $\gcd(a,n) = 1$ is necessary by supplying a counterexample with $\gcd(a,n) > 1$.

3. **Fibonacci numbers and Euclid**

   Recall that the Fibonacci numbers $F(0), F(1) \ldots$ are given by $F(0) = F(1) = 1$ and the recurrence

   $$F(n+1) = F(n) + F(n-1), \qquad n \geq 2.$$

   (a) Show that for any $n \geq 0$, $\gcd(F(n+1), F(n)) = 1$.

   (b) Show that $aF(n+1) + bF(n) = 1$, where $a = F(n-1)$ and $b = -F(n)$ if n is odd, and $a = -F(n-1)$ and $b = F(n)$ if n is even.

4. **Modular counting**

   What is the size of the the set $\{0a, 1a, 2a, 3a, \ldots, (x-1)a\}$ modulo x, if $gcd(x,a) = 4$ and $a \neq 0$? (Consider ia and ja to be the same if $ia = ja \pmod{x}$.)

5. **Modular arithmetic proof**

   Give a proof to the following theorem. You will likely find the use of modular arithmetic useful.

   Theorem. If $a_1, \ldots, a_n$ is a sequence of n integers (not necessarily distinct), prove that there is some nonempty subsequence whose sum is a multiple of n.

6. **Euclid**

   Let p, q, and r be distinct primes. Prove that there exist integers a, b, and c such that:
   $a \cdot (pq) + b \cdot (qr) + c \cdot (rp) = 1$.

7. **Modular inverse**

   Prove that the equation $ax \equiv ay \bmod n$ implies $x \equiv y \bmod n$ whenever $\gcd(a,n) = 1$. Show that the condition $\gcd(a,n) = 1$ is necessary by supplying a counterexample with $\gcd(a,n) > 1$.

8. **Binary gcd**

(a) Prove that the following statements are true for all $m, n \in \mathbb{N}$.

$$\begin{aligned}
\text{If } m \text{ is even and } n \text{ is even,} \qquad & \gcd(m,n) = 2\gcd(m/2, n/2). \\
\text{If } m \text{ is even and } n \text{ is odd,} \qquad & \gcd(m,n) = \gcd(m/2, n). \\
\text{If } m, n \text{ are both odd and } m \geq n, \qquad & \gcd(m,n) = \gcd((m-n)/2, n).
\end{aligned}$$

(b) Fill in the missing part of the following template to get an alternative algorithm for computing the gcd.

gcd(m,n):
1. If $m = 0$, return n. If $n = 0$, return m.
2. If m is even and n is even, return $2 \cdot \gcd(m/2, n/2)$.
3. If m is even and n is odd, return $\gcd(m/2, n)$.
4. If m is odd and n is even, return $\gcd(m, n/2)$.
5. ??????????.

Prove that the resulting algorithm correctly computes the gcd.