Math 309 **Fall 2022**
Homework 3 **Drew Armstrong**

---

1. Base b Arithmetic. Convert the number 123456 into base b for the following values of b:

(a) $b = 2$
(b) $b = 5$
(c) $b = 16$ [Use the letters A, B, C, D, E, F for $10, 11, 12, 13, 14, 15$.]

2. Carry the One. This problem generalizes base 10 phenomena such as

$$2749999999 + 1 = 2750000000.$$

Fix a base $b \geq 2$. Then for any integers $k, r \in \mathbb{Z}$ with $k \geq 1$ prove that

$$1 + (b-1) + (b-1)b + (b-1)b^2 + \cdots + (b-1)b^{k-1} + rb^k = (r+1)b^k.$$

[Hint: Use the geometric series $1 + b + \cdots + b^{k-1} = (b^k - 1)/(b-1)$.]

3. Lemma for the Euclidean Algorithm. Consider any positive $a, b, c, x \in \mathbb{Z}$ such that

$$a = bx + c.$$

(a) If $d \in \mathbb{Z}$ is a common divisor of b and c, show that d also divides a.
(b) If $d \in \mathbb{Z}$ is a common divisor of a and b, show that d also divides c.
(c) Combine (a) and (b) to show that $\gcd(a, b) = \gcd(b, c)$.

4. Extended Euclidean Algorithm.

(a) Find integers $x, y \in \mathbb{Z}$ such that $221x + 132y = 1$.
(b) Use your answer to solve the congruence $221c \equiv 7 \pmod{132}$ to find c. [Hint: From part (a) we have $221x \equiv 1 \pmod{132}$. Multiply both sides of $221c \equiv 7$ by x.]

5. Freshman's Dream. Let $p \geq 2$ be prime.

(a) For any integer $0 < k < p$, use Euclid's Lemma to prove that

$$\binom{p}{k} \equiv 0 \pmod{p}.$$

[Hint: We know that $p! = \binom{p}{k} k!(p-k)!$. Since p divides $p!$, Euclid's Lemma tells us that p divides $\binom{p}{k}$ or $k!(p-k)!$ If $0 < k < p-1$, show that p cannot divide $k!(p-k)!$.]

(b) For any integers $a, b \in \mathbb{Z}$, use part (a) to prove that

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

[Hint: Use the Binomial Theorem.]

6. RSA Cryptosystem. You are Eve the eavesdropper. You see that Bob sent the following message to Alice using the public key $(n, e) = (55, 27)$:

$$[2, 1, 33, 25, 1, 9, 4, 42, 25, 41, 1, 23, 23, 18, 17, 25, 1, 11].$$

Decrypt the message. [Hint: Factor $n = pq$ as a product of primes. Then find some d such that $de \equiv 1 \pmod{(p-1)(q-1)}$; using trial and error, or using Extended Euclidean Algorithm. This is the decryption exponent. After decryption, numbers $1, \ldots, 26$ stand for letters.]