**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 $10, 11, 12, 13, 14, 15$.]

I'll do them in reverse order.

(c): We divide 123456 by 16 and then repeatedly divide the quotient by 16:

$$\begin{aligned} \mathbf{123456} &= 16 \cdot \mathbf{7716} + \mathbf{0} \\ \mathbf{7716} &= 16 \cdot \mathbf{482} + \mathbf{4} \\ \mathbf{482} &= 16 \cdot \mathbf{30} + \mathbf{2} \\ \mathbf{30} &= 16 \cdot \mathbf{1} + \mathbf{14} \\ \mathbf{1} &= 16 \cdot \mathbf{0} + \mathbf{1}. \end{aligned}$$

It follows that

$$123456 = 0 + 4 \cdot 16 + 2 \cdot 16^2 + 14 \cdot 16^3 + 1 \cdot 16^4.$$

Since $E$ represents 14 we express this as

$$123456 = (1E240)_{16}.$$

(b): This time we divide 123456 by 5 and then divide each quotient by 5:

$$\begin{aligned} \mathbf{123456} &= 5 \cdot \mathbf{24691} + \mathbf{1} \\ \mathbf{24691} &= 5 \cdot \mathbf{4938} + \mathbf{1} \\ \mathbf{4938} &= 5 \cdot \mathbf{987} + \mathbf{3} \\ \mathbf{987} &= 5 \cdot \mathbf{179} + \mathbf{2} \\ \mathbf{179} &= 5 \cdot \mathbf{39} + \mathbf{2} \\ \mathbf{39} &= 5 \cdot \mathbf{7} + \mathbf{4} \\ \mathbf{7} &= 5 \cdot \mathbf{1} + \mathbf{2} \\ \mathbf{1} &= 5 \cdot \mathbf{0} + \mathbf{1}. \end{aligned}$$

We conclude that

$$123456 = (12422311)_5.$$

(a): This time I'll skip all the details:

$$123456 = (11110001001000000)_2.$$

**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 $1 + b + \cdots + b^{k-1} = (b^k - 1)/(b-1)$.]

First we remind ourselves about the geometric series:

$$\begin{aligned}(1+b+b^2+\cdots+b^{k-1})(b-1) &= (b+b^2+\cdots+b^k)-(1+b+\cdots+b^{k-1})\\ &= -1+b-b+b^2-b^2+\cdots+b^{k-1}-b^{k-1}+b^k\\ &= -1+0+0+\cdots+0+b^k\\ &= b^k-1.\end{aligned}$$

It follows (for $b \neq 1$) that[1]

$$1+b+b^2+\cdots+b^{k-1}=\frac{b^k-1}{b-1}.$$

Now we will use this to show that

$$(\ldots,r,b-1,b-1,\cdots,b-1)_b+1=(\ldots,r+1,0,0,\ldots,0)_b.$$

(Assume that $b-1$ occurs $k-1$ times.) Indeed, the left side represents the number

$$\begin{aligned}&1+[(b-1)+(b-1)b+(b-1)b^2+\cdots+(b-1)b^{k-1}+rb^k+\cdots]\\ &=1+(b-1)(1+b+b^2+\cdots+b^{k-1})+rb^k+\cdots\\ &=1+(b-1)(b^k-1)/(b-1)+rb^k+\cdots\\ &=1+(b^k-1)+rb^k+\cdots\\ &=b^k+rb^k+\cdots\\ &=(r+1)b^k+\cdots\\ &=0+0b+0b^2+\cdots+0b^{k-1}+(r+1)b^k+\cdots.\end{aligned}$$

**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 $\gcd(a,b)=\gcd(b,c)$.

(a): Suppose that $d|b$ and $d|c$, so that $b=db'$ and $c=dc'$ for some integers $b',c'\in\mathbb{Z}$. Since $a=bx+c$ it follows that

$$\begin{aligned}a&=bx+c\\ &=db'x+dc'\\ &=d(b'x+c'),\end{aligned}$$

and hence $d|a$.

(b): Suppose that $d|a$ and $d|a$, so that $a=da'$ and $b=db'$ for some integers $a',b'\in\mathbb{Z}$. Since $a=bx+c$ it follows that

$$\begin{aligned}c&=a-bx\\ &=da'-db'x\\ &=d(a'-b'x),\end{aligned}$$

and hence $d|c$.

[1]Remark: Remind yourself what happens when $|b|<1$ and $k$ goes to infinity.

(c): We have shown that the set of common divisors of $a$ and $b$ is the same as the set of common divisors of $b$ and $c$:

$$\{\text{common divisors of } a \text{ and } b\} = \{\text{common divisors of } b \text{ and } c\}.$$

It follows that the greatest element of each set is the same, i.e., 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 $x$.]

(a): We consider the set of integer triples $(x, y, r)$ satisfying $221x + 132y = r$. Beginning with the obvious triples $(1, 0, 221)$ and $(0, 1, 132)$, we perform row operations until we reach a triple of the form $(x, y, 1)$:

| $x$ | $y$ | $r$ |
|---|---|---|
| 1 | 0 | 221 |
| 0 | 1 | 132 |
| 1 | −1 | 89 |
| −1 | 2 | 43 |
| 3 | −5 | 3 |
| −43 | 72 | 1. |

Reminder of the method: Dividing 43 by 3 gives $43 = 14 \cdot 3 + 1$. Thus the row following $(-1, 2, 43)$ and $(3, -5, 3)$ is

$$(-1, 2, 43) - 14(3, -5, 3) = (-43, 72, 1).$$

We conclude that $221(-43) + 132(72) = 1$. Note: This solution is **not unique**. Since $221(132k) + 132(-221k) = 0$ for any $k$, we also have

$$221(-43 + 132k) + 132(72 - 221k) = 1 \quad \text{for any } k \in \mathbb{Z}.$$

(b): Since $132 \equiv 0 \pmod{132}$, the result from part (a) tells us that

$$1 \equiv 221(-43) + 132(72) \equiv 221(-43) + 0(72) \equiv 221(-43) \pmod{132}.$$

In other words, we can kill 221 (mod 132) by multiplying by −43 (mod 132), which in standard form is 89 (mod 132). That is, we have

$$221 \cdot 89 \equiv 221 \cdot (-43) \equiv 1 \pmod{132}.$$

Thus, to solve the congruence $221c \equiv 7 \pmod{132}$ we should multiply both sides by 89:

$$\begin{aligned} 221c &\equiv 7 \\ 89 \cdot 221c &\equiv 89 \cdot 7 \\ 1c &\equiv 623 \\ c &\equiv 95 \pmod{132}. \end{aligned}$$

This answer is unique mod 132, but it represents infinitely many integer solutions:

$$\begin{aligned} c &= (\text{any integer that is congruent to 95 mod 132}) \\ &= (\text{any integer of the form } 95 + 132k \text{ for some integer } k \in \mathbb{Z}). \end{aligned}$$

**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.]

(a): Let $p \geq 2$ be prime and consider any integer $0 < k < p$. The binomial coefficient $\binom{p}{k}$ satisfies the equation

$$\begin{aligned} p! &= \binom{p}{k} k!(p-k)! \\ p(p-1)\cdots 3 \cdot 2 \cdot 1 &= \binom{p}{k} k(k-1)\cdots 3\cdot 2\cdot 1\cdot (p-k)(p-k-1)\cdots 3\cdot 2\cdot 1. \end{aligned}$$

Since $p$ divides the left hand side, it must also divide the right hand side:

$$p \,\Big|\, \binom{p}{k} k(k-1)\cdots 3\cdot 2\cdot 1\cdot (p-k)(p-k-1)\cdots 3\cdot 2\cdot 1$$

Since $p$ is prime, Euclid's Lemma[2] tells us that $p$ must divide one of the factors on the right hand side. However, since $0 < k < p$, every factor on the right hand side is smaller than $p$, except for $\binom{p}{k}$. Since $p$ cannot divide a number that is smaller than itself, we conclude that $p$ divides $\binom{p}{k}$, which is equivalent to saying that

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

(b): Let $p \geq 2$ be prime and consider any two integers $a, b \in \mathbb{Z}$. Then from part (a) and the Binomial Theorem we have

$$\begin{aligned} (a+b)^p &\equiv a^p + \binom{p}{1} a^{p-1}b + \binom{p}{2} a^{p-2}b^2 + \cdots + \binom{p}{p-1} ab^{p-1} + b^p \\ &\equiv a^p + 0a^{p-1}b + 0a^{p-2}b^2 + \cdots + 0ab^{p-1} + b^p \\ &\equiv a^p + b^p \pmod{p}. \end{aligned}$$

**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.]

---

[2] Recall: If $p$ is prime then Euclid's Lemma says that $p|ab$ implies $p|a$ or $p|b$.

Notice that $n = 55$ factors as $n = pq = 5 \cdot 11$, where $p = 5$ and $q = 11$ are prime. There, we broke the system.[3] Next we need to find the decryption exponent. Recall that $d$ satisfies

$$de + (p-1)(q-1)k = 1,$$

for some integer $k$ whose value we don't care about. Since $e = 27$ and $(p-1)(q-1) = 40$ we want to find integers $d, k \in \mathbb{Z}$ such that

$$40k + 27d = 1,$$

and this can be done with the Extended Euclidean Algorithm:

| $k$ | $d$ | $r$ |
|---|---|---|
| 1 | 0 | 40 |
| 0 | 1 | 27 |
| 1 | $-1$ | 13 |
| $-2$ | 3 | 1. |

We conclude that $27(3) + 40(-2) = 1$, hence we can take $d = 3$ as the decryption exponent.

To encrypt a message $0 \leq m < 55$, Bob computes $c = m^{27} \pmod{55}$. Then to decrypt Bob's message we compute $c^3 \pmod{55}$. The standard representative of $c^3 \pmod{55}$, i.e., the representative between 0 and 54, is guaranteed to equal $m$. Here is Bob's encrypted message:

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

Raising each integer to the power of 3 and then reducing mod 55 gives

$$[8, 1, 22, 5, 1, 14, 9, 3, 5, 6, 1, 12, 12, 2, 18, 5, 1, 11],$$

which corresponds to the message

$$[h, a, v, e, a, n, i, c, e, f, a, l, l, b, r, e, a, k].$$

[3] If $p$ and $q$ were very large we would not be able to factor $n = pq$.