Math 230 **Fall 2018**
Exam 3 — Tues Dec 4 **Drew Armstrong**

No communication devices or notes are allowed. Any student caught cheating will receive a score of zero. Each of the 4 problems is worth 6 points, for a total of 24 points.

Problem 1.

(a) Use the Extended Euclidean Algorithmn to compute the inverse of 10 mod 17.

Consider the set of triples $(k, \ell, m) \in \mathbb{Z}^3$ such that $10k + 17\ell = m$. Beginning with $(0, 1, 17)$ and $(1, 0, 10)$ we have the following table:

k	ℓ	m
0	1	17
1	0	10
-1	1	7
2	-1	3
-5	3	1

It follows that $10 \cdot (-5) = 1$ mod 17 and hence $10^{-1} = -5 = 12$ mod 17.

(b) Use your answer from (a) to solve the equation $10x = 8$ mod 17.

Dividing by 10 is the same as multiplying by 12. Thus we have

$$\begin{aligned} 10x &= 8 \\ x &= 8 \cdot 12 \\ x &= 96 \\ x &= 11 \text{ mod } 17. \end{aligned}$$

(c) Compute 16^{16} mod 17. You may assume that Fermat's Little Theorem is true.

Fermat's Little Theorem says that $a^{p-1} = 1$ mod p for all $a, p \in \mathbb{Z}$ with p prime and $p \nmid a$. Taking $a = 16$ and $p = 17$ gives

$$16^{16} = 1 \text{ mod } 17.$$

Problem 2. Let $\sim$ be an equivalence relation on a set S.

(a) Accurately state the three axioms that $\sim$ must satisfy.

(E1) $\forall x \in S, x \sim x$,
(E2) $\forall x, y \in S, x \sim y \Rightarrow y \sim x$,
(E3) $\forall x, y, z \in S, (x \sim y \wedge y \sim z) \Rightarrow x \sim z$.

(b) For all $x \in S$ let $[x] := \{z \in S : x \sim z\}$. Prove that $[x] = [y]$ implies $x \sim y$.

Assume that $[x] = [y]$. Then from (E1) we have $y \in [y] = [x]$, which implies that $x \sim y$.

(c) Continuing from (b), prove that $x \sim y$ implies $[x] = [y]$.

Assume that $x \sim y$, so (E2) implies $y \sim x$. To prove that $[x] \subseteq [y]$, suppose that $z \in [x]$, which means that $x \sim z$. Then from (E3) we have $(y \sim x \wedge x \sim z) \Rightarrow y \sim z$ and hence $z \in [y]$. To prove that $[y] \subseteq [x]$, suppose that $z \in [y]$, which means that $y \sim z$. Then from (E3) we have $(x \sim y \wedge y \sim z) \Rightarrow x \sim z$ and hence $z \in [x]$.

Problem 3. Fix an integer $n \in \mathbb{Z}$ and for all integers $a, b \in \mathbb{Z}$ consider the relation

$$a \sim_n b \iff n|(a-b).$$

(a) Prove that $\sim_n$ is an equivalence relation on $\mathbb{Z}$.

(E1) For all $a \in \mathbb{Z}$ we have $n \cdot 0 = (a-a)$, hence $n|(a-a)$, hence $a \sim_n a$.
(E2) Consider $a, b \in \mathbb{Z}$ with $a \sim_n b$, so that $a - b = nk$ for some $k \in \mathbb{Z}$. Then $(b-a) = n(-k)$ implies that $n|(b-a)$ and hence $b \sim_n a$.
(E3) Consider $a, b, c \in \mathbb{Z}$ with $a \sim_n b$ and $b \sim_n c$. This means that $a - b = nk$ and $b - c = n\ell$ for some $\ell \in \mathbb{Z}$. But then we have

$$a - c = (a-b) + (b-c) = nk + n\ell = n(k+\ell),$$

which implies that $n|(a-c)$, hence $a \sim_n c$.

(b) For all $a \in \mathbb{Z}$ define the set $[a]_n = \{c \in \mathbb{Z} : a \sim_n c\}$. Prove that $[a]_n = [a']_n$ and $[b]_n = [b']_n$ imply $[a+b]_n = [a'+b']_n$.

Assume that $[a]_n = [a']_n$ and $[b]_n = [b']_n$. From Problem 2(b) and the definition of $\sim_n$ this means that $a - a' = nk$ and $b - b' = n\ell$ for some $k, \ell \in \mathbb{Z}$. But then we have

$$(a+b) - (a'+b') = (a-a') + (b-b') = nk + n\ell = n(k+\ell),$$

which implies that $(a+b) \sim_n (a'+b')$. Then Problem 2(c) implies $[a+b]_n = [a'+b']_n$.

(c) Continuing from (b), prove that $[a]_n = [a']_n$ and $[b]_n = [b']_n$ imply $[ab]_n = [a'b']_n$.

Assume that $[a]_n = [a']_n$ and $[b]_n = [b']_n$. From Problem 2(b) and the definition of $\sim_n$ this means that $a - a' = nk$ and $b - b' = n\ell$ for some $k, \ell \in \mathbb{Z}$. But then we have

$$\begin{aligned} ab - a'b' &= ab - (a-nk)(b-n\ell) \\ &= \cancel{ab} - (\cancel{ab} - an\ell - bnk + n^2k\ell) \\ &= n(a\ell + bk - nk\ell), \end{aligned}$$

which implies that $ab \sim_n a'b'$. Then Problem 2(c) implies $[ab]_n = [a'b']_n$.

Problem 4. Fix integers $a, b, n \in \mathbb{Z}$ and for all $k \in \mathbb{Z}$ consider the following statement:

$$P(k) = \text{“} [a^k]_n = [b^k]_n. \text{”}$$

(a) Accurately state the Principle of Induction.

Let $P(n)$ be a statement depending on an integer $n \in \mathbb{Z}$. Suppose that

$$\begin{cases} \bullet\ P(b) \text{ is true for some specific } b \in \mathbb{Z}, \text{ and} \\ \bullet\ \text{for all } n \geq b \text{ we have } P(n) \Rightarrow P(n+1). \end{cases}$$

Then it follows that $P(n)$ is true for all $n \geq b$.

(b) Assuming that $P(1)$ is true, use induction to prove that $P(k)$ is true for all $k \geq 1$. [Hint: You can use the result of Problem 3(c).]

Let $[a]_n = [b]_n$, i.e., $P(1)$ is true. Now assume for induction that $[a^k]_n = [b^k]_n$, i.e., $P(k)$ is true. Then since $[a]_n = [b]_n$ and $[a^k]_n = [b^k]_n$ it follows from Problem 3(c) that

$$\begin{aligned} [a \cdot a^k]_n &= [b \cdot b^k]_n \\ [a^{k+1}]_n &= [b^{k+1}]_n. \end{aligned}$$

In other words, $P(k+1)$ is true. It follows by induction that $P(k)$ is true for all $k \geq 1$.

Alternate Proof. For all $k \geq 1$ note that

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

It follows that $n|(a-b)$ implies $n|(a^k - b^k)$.

Math 230 D **Fall 2015**
Exam 3 — Mon Dec 7 **Drew Armstrong**

There are 4 problems, worth 6 points each, for a total of 24 points. This is a closed book test. Anyone caught cheating will receive a score of **zero**.

Problem 1. Hand Computations.

(a) Use Pascal's Triangle to compute the expansion of $(1+x)^5$.

Here is Pascal's Triangle:

$$\begin{array}{ccccccccccc} & & & & & 1 & & & & & \\ & & & & 1 & & 1 & & & & \\ & & & 1 & & 2 & & 1 & & & \\ & & 1 & & 3 & & 3 & & 1 & & \\ & 1 & & 4 & & 6 & & 4 & & 1 & \\ 1 & & 5 & & 10 & & 10 & & 5 & & 1 \end{array}$$

Thus we conclude that

$$(1+x)^5 = 1 + 5x + 10x^2 + 10x^3 + 5x^4 + x^5.$$

(b) Compute the standard form of $\left[\frac{7!}{3!4!}\right]_7$.

$$\left[\frac{7!}{3!4!}\right]_7 = \left[\frac{7\cdot 6\cdot 5\cdot \cancel{4\cdot 3\cdot 2\cdot 1}}{3\cdot 2\cdot 1\cdot \cancel{4\cdot 3\cdot 2\cdot 1}}\right]_7 = [35]_7 = [0]_7.$$

(c) Compute the standard form of $\left[2^6\right]_7$.

$$[2^6]_7 = [2^3]_7 \cdot [2^3]_7 = [8]_7 \cdot [8]_7 = [1]_7 \cdot [1]_7 = [1]_7.$$

Problem 2. Modular Arithmetic. Let $0 \neq n \in \mathbb{Z}$. Define the set $\mathbb{Z}/n := \{[a]_n : a \in \mathbb{Z}\}$ with equivalence relation $[a]_n = [b]_n \Leftrightarrow n|(a-b)$ and algebraic operations

$$[a]_n + [b]_n := [a+b]_n \qquad \text{and} \qquad [a]_n \cdot [b]_n := [ab]_n.$$

(You can assume that this is all well-defined.) Recall that $\mathbb{Z}/n$ is a ring with additive identity element $[0]_n$ and multiplicative identity element $[1]_n$.

(a) If $\gcd(a,n) = 1$, prove that the element $[a]_n \in \mathbb{Z}/n$ has a multiplicative inverse. [You can assume Bézout's Lemma.]

Proof. Since $\gcd(a,n) = 1$, Bézout's Lemma says that there exist $x, y \in \mathbb{Z}$ with $ax + ny = 1$. Then we have

$$1 - ax = ny \implies n|(ax-1) \implies [1]_n = [ax]_n = [a]_n \cdot [x]_n.$$

It follows that the inverse exists:

$$[a^{-1}]_n = [x]_n.$$

□

(b) If the element $[a]_n \in \mathbb{Z}/n$ has a multiplicative inverse, prove that there exist $x, y \in \mathbb{Z}$ with $ax + ny = 1$.

Proof. Suppose there exists $x \in \mathbb{Z}$ with $[a]_n \cdot [x]_n = [1]_n$. Then we have

$$[1]_n = [ax]_n \quad \Longrightarrow \quad n|(1-ax) \quad \Longrightarrow \quad 1 - ax = ny \text{ for some } y \in \mathbb{Z}.$$

□

(c) If there exist $x, y \in \mathbb{Z}$ with $ax + ny = 1$, prove that $\gcd(a, n) = 1$.

Proof. Suppose that $ax + ny = 1$ for some $x, y \in \mathbb{Z}$ and let $d \in \mathbb{Z}$ be **any** common divisor of a and b, say $a = dk$ and $b = d\ell$ for some $k, \ell \in \mathbb{Z}$. Then we have

$$1 = ax + by = (dk)x + (d\ell)y = d(kx + \ell' y),$$

which implies that $d = \pm 1$. It follows that the greatest common divisor is 1. □

Problem 3. Principle of Induction.

(a) Accurately state the Principle of Induction.

Let $P(n)$ be a statement depending on an integer $n \in \mathbb{Z}$. Suppose that

$$\begin{cases} \bullet\ P(b) \text{ is true for some specific } b \in \mathbb{Z}, \text{ and} \\ \bullet\ \text{for all } n \geq b \text{ we have } P(n) \Rightarrow P(n+1). \end{cases}$$

Then it follows that $P(n)$ is true for all $n \geq b$.

(b) For all integers $n \geq 2$ define the statement $P(n) :=$ "$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$". Prove that $P(2)$ is a true statement.

$$1 + 2 = \frac{2 \cdot 3}{2}$$

(c) Now fix an integer $k \geq 2$ and assume for induction that $P(k)$ is true. In this case, prove that $P(k+1)$ is also true.

Proof. Fix an integer $k \geq 2$ and assume for induction that $P(k)$ is true. In other words, assume that

$$1 + 2 + \cdots + k = \frac{k(k+1)}{2}.$$

Then it follows that

$$\begin{aligned} 1 + 2 + \cdots + (k+1) &= (1 + 2 + \cdots + k) + (k+1) \\ &= \frac{k(k+1)}{2} + (k+1) \\ &= \left(\frac{k}{2} + 1\right)(k+1) \\ &= \frac{(k+2)}{2}(k+1) \\ &= \frac{(k+1)((k+1)+1)}{2}. \end{aligned}$$

In other words, $P(k+1)$ is true. □

Problem 4. Binomial Theorem.

(a) Accurately state the Binomial Theorem.

For all integers $a, b, n \in \mathbb{Z}$ with $n \geq 0$ we have

$$(a+b)^n = \sum_{k=0}^{n} \frac{n!}{k!(n-k)!} a^k b^{n-k}.$$

(b) Let $k, p \in \mathbb{Z}$ with p prime and $1 \leq k \leq p-1$. In this case you can assume that p divides the integer $\frac{p!}{k!(p-k)!}$. Use this fact together with the Binomial Theorem to prove that for all $a, b \in \mathbb{Z}$ we have $[(a+b)^p]_p = [a^p + b^p]_p$.

Proof. When $1 < k < p$ we have assumed that

$$\left[\frac{p!}{k!(p-k)!}\right]_p = [0]_p.$$

Then using the Binomial Theorem gives

$$\begin{aligned}
[(a+b)^p]_p &= \left[a^p + \sum_{k=1}^{p-1} \frac{p!}{k!(p-k)!} a^k b^{p-k} + b^p\right]_p \\
&= [a^p]_p + \sum_{k=1}^{p-1} \left[\frac{p!}{k!(p-k)!}\right]_p \cdot [a^k b^{p-k}]_p + [b^p]_p \\
&= [a^p]_p + \sum_{k=1}^{p-1} [0]_p \cdot [a^k b^{p-k}]_p + [b^p]_p \\
&= [a^p]_p + \sum_{k=1}^{p-1} [0]_p + [b^p]_p \\
&= [a^p]_p + [0]_p + [b^p]_p \\
&= [a^p]_p + [b^p]_p.
\end{aligned}$$

$\square$