Math 780/780I **Test 2** Name: Answer Key.

1. The positive integer n when written in base 10 has last digit 8 and the sum of its the digits is 15. Explain briefly why n is divisible by 6.

Solution: As the last digit is 8 the number n is even, that is $2 \mid n$. As the sum of the digits is 15, which is divisible by 3, we have that n is also divisible by 3. Thus $2 \mid n$ and $3 \mid n$. As $\gcd(2,3)=1$, this implies $2 \cdot 3 = 6 \mid n$. □

2. Find the general solution to the Diophantine equation

$$10x + 8y = 22.$$

Solution: As $\gcd(10,8) = 2 \mid 22$ we see that this has a solution. We first look for a solution to

$$10x + 8y = \gcd(8,10) = 2.$$

This can be done by the Euclidean algorithm, but it is easy to see that $x = 1$, $y = -1$ is a solution, that is

$$10(1) + 8(-1) = 2.$$

Multiply this through by 11 to get

$$10(11) + 8(-11) = 22.$$

So $(x_0, y_0) = (11, -11)$ is a particular solution. Thus the general solution is

$$x = x_0 + \frac{8}{2}t = 11 + 4t$$

$$y = y_0 - \frac{10}{2}t = -11 - 5t$$

where t is any integer. □

3. How many integer solutions (x, y) to

$$4x + 3y = 200.$$

have both x and y positive?

Solution: We first find a particular solution to $4x + 3y = \gcd(4,3) = 1$. Such a solution is $x = 1$, $y = -1$. Thus

$$4(1) + 3(-1) = 1.$$

Multiply by 200 to get

$$4(200) + 3(-200) = 200.$$

The general solution to this is

$$x = 200 - 3t$$

$$y = -200 + 4t$$

where t can be any integer. We are only interested in positive solutions so we want

$$x = 200 - 3t > 0 \quad \Longrightarrow \quad t < \frac{200}{3} = 66.6666\ldots$$

$$y = -200 + 4t > 0 \quad \Longrightarrow \quad t > \frac{200}{4} = 50$$

As t is an integer this gives $51 \le t \le 66$. The number of t's satisfying this is $66 - 51 + 1 = 16$ which is also the number of positive solutions to $4x + 3y = 200$. □

4. For the integers $a = 44$ and $b = 28$ find integers x and y such that

$$ax + by = \gcd(a,b)$$

by use of the Euclidean algorithm.

Solution: So start:

$$\begin{aligned}(16) &= (44) - (28)\\(12) &= (26) - (16)\\(4) &= (16) - (12)\end{aligned}$$

Now back solve

$$\begin{aligned}(4) &= (16) - (12)\\&= (16) - \big((26) - (16)\big)\\&= -(26) + 2(16)\\&= -(26) + 2\big((44) - (28)\big)\\&= 2(44) - 3(28)\end{aligned}$$

Therefore $x = 2$ and $y = -3$ work. □

5. Find the general solution to $x + 2y + 3z = 12$.

Solution: Rewrite as

$$x + 2y = 12 - 3z.$$

We first find a particular solution to $x + 2y = 1$. One such solution is $(x, y) = (-1, 1)$. Multiply

$$(-1) + 2(1) = 1$$

by $12 - 3z$ to get

$$(-12 + 3z) + 2(12 - 3z) = 12 - 3z.$$

The general solution to this is

$$x = -12 + 3z + 2t, \qquad y = 12 - 3z - t$$

So if we let $z = s$ we find the general solution to our original system is

$$\begin{aligned}x &= -12 + 3s + 2t\\y &= 12 - 3s - t\\z &= s\end{aligned}$$

where $s, t \in \mathbb{Z}$. □

6. (a) State Bézout's theorem.

Solution: For all integers a and b, not both zero, there are integers x and y such that

$$ax + by = \gcd(a, b).$$

□

(b) Use Bézout's theorem to prove that if $\gcd(a, b) \mid c$, then $ax + by = c$ has solutions in integers.

Solution: Let $d = \gcd(a, b)$. Then $d \mid c$ so there is an integer c' such that $c = c'd$. By Bézout's Theorem there are integers x_0 and y_0 such that $ax_0 + by_0 = d$ Multiply this by c' to get

$$a(c'x_0) + b(c'y_0) = c'd = c.$$

Thus $ax + by = c$ has the solution $(x, y) = (c'x_0, c'y_0)$. □

7. Define $a \equiv b \mod n$.

Solution: $n \mid (b - a)$ □

(a) Prove that if $a \equiv b \mod n$ and $c \equiv d \mod n$, then $a + c \equiv b + d \mod n$.

Solution: The hypothesis is that $n \mid (b - a)$ and $n \mid (d - c)$. Thus there are integers k and ℓ such that $(b - a) = kn$ and $(d - c) = \ell n$. Whence

$$(b + d) - (a + c) = (b - a) + (d - c) = kn + \ell n = (k + \ell)n$$

which shows that $n \mid \big((b + d) - (a + c)\big)$, and therefore $a + c \equiv b + d \mod n$. □

(b) Let k and n be positive integers. Show

$$ak \equiv bk \mod nk \qquad \Longrightarrow \qquad a \equiv b \mod n.$$

Solution: If $ak \equiv bk \mod nk$, then $nk \mid (bk - ak)$ which in turn implies there is an integer ℓ such that

$$(bk - ak) = nk\ell.$$

We cancel k in this equality to get $(b - a) = n\ell$ which implies $n \mid (b - a)$. That is $a \equiv b \mod n$. □

8. State both forms of Fermat's Little Theorem. (Which order you do this does not matter.)
(a) *Form 1:*

Solution: If p is a prime and $\nmid a$, then $a^{p-1} \equiv 1 \mod p$. □

(b) *Form 2:*

Solution: If p is a prime then for any integer a we have $a^p \equiv a \mod p$. □

(c) Use Fermat's Little Theorem to find the remainder when 7^{38} is divided by 13.

Solution: By Fermat's Little Theorem we know that $7^{12} \equiv 1 \mod 13$. Therefore

$$7^{38} = \left(7^{12}\right)^3 \cdot 7^2 \equiv 1^2 \cdot 7^2 \equiv 49 \equiv 10 \mod 13.$$

So the remainder is 10. □

9. Let n be a positive integer.
(a) Define what it means for $\widehat{a}$ to be the inverse of a modulo n.

Solution: This means that $\widehat{a}a \equiv 1 \mod n$. □

(b) If $\gcd(a, n) = 1$ prove that a has an inverse modulo n.

Solution: As $\gcd(a, n) = 1$ Bézout's Theorem tells us there are integers x and y such that

$$ax + ny = 1.$$

If we view this equation $\mod n$ we get

$$ax \equiv 1 \mod n.$$

Thus $\widehat{a} = x$ is an inverse of a modulo n. □

10. It can be shown that $3^{100} \equiv 1 \mod 5$ and $3^{100} \equiv 4 \mod 7$. What is the remainder when 3^{100} is divided by $35 = 5 \cdot 7$. *Hint:* Chinese Remainder Theorem.

Solution: If $x = 3^{100}$ then x is a solution to the Chinese remainder problem

$$x \equiv 1 \mod 5$$
$$x \equiv 4 \mod 7$$

We use our method for solving these problems. An inverse of 7 modulo 5 is 3 (as $3 \cdot 7 = 21 \equiv 1 \mod 5$). An inverse of 5 modulo y is 3 (as $3 \cdot \cdot \cdot 5 = 15 \equiv 1 \mod 7$). So

$$x = 7 \cdot 3 \cdot 1 + 5 \cdot 3 \cdot 4 = 21 + 60 = 81$$

is a solution and this solution is unique modulo 35. Reducing 81 modulo 35 we have

$$81 \equiv 11 \mod 35$$

and therefore the remainder of 3^{100} when divided by 35 is 11. □