

College of the Holy Cross, Fall 2008
Math 243, Practice Midterm 1

1. (a) There is an integer c such that $b = ac$.
(b) Assume that $a|b$ and $b|c$. This means that there exist integers d and e with $a = db$ and $b = ce$. Substituting the second equation into the first gives $a = d(ce)$, and thus $a = c(de)$. Therefore a divides c .
2. First, check that the statement holds for $n = 1$. Indeed, $3|(1^3 + 2 \cdot 1 = 3)$.
Now assume that $3|(k^3 + 2k)$, which means that $k^3 + 2k = 3q$ for some integer q . This is our inductive hypothesis.

Now we must show that $3 | [(k + 1)^3 + 2(k + 1)]$.

Proof:

$$(k + 1)^3 + 2(k + 1) = k^3 + 3k^2 + 3k + 1 + 2k + 2 = (k^3 + 2k) + 3k^2 + 3k + 3.$$

By the inductive hypothesis, $k^3 + 2k = 3q$, so the rightmost expression above becomes

$$3(q + k^2 + k + 1)$$

This is divisible by 3, which is what we wanted to show. QED

3.

$$\begin{aligned} 5088 &= 156 \cdot 32 + 96 \\ 156 &= 96 \cdot 1 + 60 \\ 96 &= 60 \cdot 1 + 36 \\ 60 &= 36 \cdot 1 + 24 \\ 36 &= 24 \cdot 1 + 12 \\ 24 &= 12 \cdot 2 + 0 \end{aligned}$$

Therefore the greatest common divisor of 5088 and 156 is 12.

4. We can subtract 19 from both sides of the congruence to get

$$9x \equiv -17 \pmod{23}$$

We need to find s and t such that $1 = 9s + 23t$. Do this using the Euclidean algorithm:

$$\begin{aligned}
23 &= 9 \cdot 2 + 5 \\
9 &= 5 \cdot 1 + 4 \\
5 &= 4 \cdot 1 + 1 \\
1 &= 1 \cdot 1 + 0
\end{aligned}$$

Now rearrange each of these:

$$\begin{aligned}
5 &= 23 \cdot 1 + (-2) \cdot 9 \\
4 &= 9 \cdot 1 + (-1) \cdot 5 \\
1 &= 5 \cdot 1 + (-1) \cdot 4
\end{aligned}$$

Now we substitute successively:

$$\begin{aligned}
1 &= 1 \cdot 5 + (-1) \cdot 4 \\
&= 1 \cdot 5 + (-1) \cdot (9 \cdot 1 + (-1) \cdot 5) \\
&= 2 \cdot 5 + (-1) \cdot 9 \\
&= (2) \cdot (23 + (-2) \cdot 9) + (-1) \cdot 9 \\
&= (2) \cdot 23 + (-5) \cdot 9
\end{aligned}$$

So $s = -5$ and $t = 2$. This tells us that $-5 \cdot 9 \equiv 1 \pmod{23}$. Multiplying both sides by -17 gives

$$85 \cdot 9 \equiv -17 \pmod{23}.$$

Therefore $x = 85$. Indeed, any number congruent to 85 modulo 23 will do, so we take $x = 85 - 3 \cdot 23 = 16$.

5. [1], [7], [11], [13], [17], [19], [23], [29]. To find the inverse of [23], you can use the Euclidean algorithm to find s and t with $1 = 23s + 30t$, as done in the previous problem. This process yields

$$1 = 23 \cdot 17 + (-13 \cdot 30).$$

Thus $[23]^{-1} = [17]$.

6. Let's suppose that $x \in \mathbb{Z}$ is a solution to the congruence, i.e., that $x^2 \equiv 2 \pmod{3}$. We will derive a contradiction.

Using the division algorithm, we can write x as $3q + r$, where q and r are integers and $0 \leq r < 3$. Thus we have three cases:

Case 1: $r = 0$. Then $x = 3q$. So $x^2 = 9q^2$. This means that x^2 is a multiple of 3, so $x^2 \equiv 0 \pmod{3}$. Therefore x is not a solution to $x^2 \equiv 2 \pmod{3}$.

Case 2: $r = 1$. Then $x = 3q + 1$. So $x^2 = 9q^2 + 6q + 1$. This means that $x^2 - 1$ is a multiple of 3, so by the definition of equivalence modulo 3, $x^2 \equiv 1 \pmod{3}$. Therefore x is not a solution to $x^2 \equiv 2 \pmod{3}$.

Case 2: $r = 2$. Then $x = 3q + 2$. So $x^2 = 9q^2 + 12q + 4$. This means that $x^2 - 1 = 9q^2 + 12q + 3$, and this is a multiple of 3. As in Case 2, this means $x^2 \equiv 1 \pmod{3}$. Therefore x is not a solution to $x^2 \equiv 2 \pmod{3}$.

Thus in all cases x is not a solution to $x^2 \equiv 2 \pmod{3}$. This contradicts our initial assumption that x was a solution to this equation. QED

7. Suppose that $ax \equiv b \pmod{n}$ has a solution. This means that there exists an $x \in \mathbb{Z}$ such that $ax \equiv b \pmod{n}$, which is equivalent to saying that $n|(ax - b)$. Hence there exists $c \in \mathbb{Z}$ such that $cn = ax - b$. Therefore

$$b = ax - cn.$$

Now d is the greatest common divisor of a and n , so $d|a$ and $d|n$ (this is part of the definition of greatest common divisor). Thus there exist ℓ and m with $a = \ell d$ and $n = md$. Thus our equation becomes

$$b = \ell dx - cmd = d(\ell x - cm).$$

Hence d divides b . QED

8. Suppose that $[x] \in \mathbb{Z}_p$ is its own multiplicative inverse. This means that $[x][x] = [1]$, or in other words

$$[x^2] = [1].$$

This in turn means that $x^2 \equiv 1 \pmod{p}$, which is the same as $x^2 - 1 \equiv 0 \pmod{p}$. This means that $p|(x^2 - 1)$.

We can factor $x^2 - 1$ as $(x - 1)(x + 1)$, and this gives us

$$p|(x - 1)(x + 1). \tag{1}$$

We now apply Euclid's Lemma, which says that if a and b are any integers and $p|ab$, then either $p|a$ or $p|b$. In our situation, applying this to (1) gives that either $p|(x - 1)$ or $p|(x + 1)$. This means that either $x - 1 \equiv 0 \pmod{p}$ or $x + 1 \equiv 0 \pmod{p}$. This, in turn, means that $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$. Thus $[x] = [1]$ or $[x] = [-1]$. QED