Chapter 4.1: Modular Arithmetic

Wednesday, July 8

Divisibility Recap

1. Using the fact that 1 is the smallest positive integer, prove that if $a|b$ (and b $\neq 0$) then $|a| \leq |b|$.

   If 1 is the smallest integer then $k \geq 1$ for any $k \in \mathbb{Z}^+$, so $|k| \geq 1$ for any $k \neq 0$. Multiplying by $|a|$ makes the inequality $|ak| \geq |a|$. If $a|b$ and $b \neq 0$ then there is some $k \neq 0$ so that $ak = b$. Taking absolute values and combining with the previous inequality gives the result $|a| \leq |ak| = |b|$, so $|a| \leq |b|$.

2. Prove that if $a|b$ and $b|a$ then $|a| = |b|$ (or, $a = \pm b$).

   Since $a|b$, $|a| \leq |b|$. Since $b|a$, $|b| \leq |a|$. Therefore, $|a| = |b|$.

Modular Arithmetic

Evaluate the following:

1. $44 \pmod 3 = 2$

2. $171 \pmod{12} = 51 \pmod{12} = 3$

3. $-26 \pmod 5 = 4$

4. $199^2 \pmod 5 = 9^2 \pmod 5 = 81 \pmod 5 = 1$

5. $(2301 \pmod 3)^2 \pmod 5 = 0^2 \pmod 5 = 0$

6. $23^{88} \pmod 2 = 1^8 8 \pmod 2 = 1$

7. $2^{100} \pmod{10}$

   One method: observe that $2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 6, 2^5 \equiv 2 \pmod{10}, 2^6 \equiv 4 \pmod{10} \ldots$ guess that the last digits follow the pattern 2-4-8-6, with period 4. Since 100 is divisible by 4, the last digit should be 6. (WARNING: this is not rigorous! It is just a nice way to start, since showing that you have the right answer is often easier once you know what that answer should be)

   Trying to show that this pattern works, we could say that $6 \cdot 6 = 36 \equiv 6 \pmod{10}$, so $2^{100} \pmod{10} = (2^4)^{25} \pmod{10} \equiv 6^2 5 \pmod{10} \equiv 6 \pmod{10}$, since 6 raised to any larger power should still be 6 mod 10.

   Another method: 2^{100} is even. Also, $2^4 \equiv 1 \pmod 5$, so $2^{100} \equiv 1 \pmod 5$. This means that 2^{100} mod 10 is equal to 1 or 6, and since it is even it must be 6.

8. $2737 \cdot 8184 \pmod 9$

   Use the fact that 27 and 81 are both divisible by 9, so 2700 and 8100 are both divisible by 9.

   $2737 \cdot 8184 \equiv 37 \cdot 84 \equiv 1 \cdot 3 \equiv 3 \pmod 9$.

9. $2^{64} \pmod{13}$

   $2^6 = 64 \equiv (-1) \pmod{13}$, so $2^{12} \equiv 1 \pmod{13}$, so $2^{12 \cdot 5} = 2^{60} \equiv 1 \pmod{13}$. Therefore $2^{64} = 2^{60} \cdot 2^4 \equiv 3 \pmod{13}$.

10. $88^5 \pmod{90}$

    $88^5 \equiv (-2)^5 \equiv -32 \equiv 58 \pmod{90}$.

11. $97 \cdot 85 \pmod{100}$

$$97 \cdot 85 \equiv (-3) \cdot (-15) \equiv 45 \pmod{100}$$

12. $155 \cdot 822 \pmod{10}$

$$155 \cdot 822 \equiv 5 \cdot 2 \equiv 0 \pmod{10}$$

Squares

1. Prove that an integer a is divisible by 5 if and only if a^2 is divisible by 5 (proof by cases).

   If $a = 5k$ is divisible by 5 then $a^2 = 5ka$ is clearly divisible by 5.

   If $a \equiv 1, 2, 3, 4 \pmod{5}$ then $a^2 \equiv 1, 4, 4, 1 \pmod{5}$. In none of these cases is a^2 divisible by 5, so if a is not divisible by 5 then neither is a^2.

2. Prove that an integer a^2 is divisible by 3 if and only if it is divisible by 9.

   Break into cases based on whether a is divisible by 3. If a is divisible by 3, then a^2 is divisible by 3 and 9.

   If a is not divisible by 3, then a^2 is not divisible by 3 or 9.

3. Prove that 98765432 is not a perfect square.

   The last digit is 2, and any square number will be $0, 1, 4, 9, 6,$ or 5 mod 10 (check by cases). Therefore this number cannot be a perfect square.

4. Using the fact that $n^2 \equiv 0$ or $n^2 \equiv 1 \pmod{4}$, prove that 111111 cannot be written as the sum of any two square numbers (what are the possibilities for $a^2 + b^2 \pmod{4}$?)

   The only possibilities for $a^2 + b^2 \pmod{4}$ are $0 + 0 = 1$, $0 + 1 = 1$, and $1 + 1 = 2$. Therefore there are no numbers $a, b \in \mathbb{Z}$ such that $a^2 + b^2 \equiv 3 \pmod{4}$. Since 111111 is equivalent to 3 mod 4, it cannot be written as the sum of two squares.

Method of Nines

1. Use the Method of Nines to show that $35121 \cdot 87122 \neq 3059911762$.

   $3 + 5 + 1 + 2 + 1 = 12 \equiv 3 \pmod{9}$ and $8 + 7 + 1 + 1 + 2 + 2 = 20 \equiv 2 \pmod{9}$, so the answer should be 6 mod 9.

   But $3 + 0 + 5 + 9 + 9 + 1 + 1 + 7 + 6 + 2 = 43 \equiv 7 \pmod{9}$, so it cannot be the right answer.

2. Find an example of an error in a multiplication problem that the Method of Nines fails to catch.

   The Method of Nines will not catch the error in $3 \cdot 3 = 27$.

The Trouble With Division in $\mathbb{Z}_m$

1. Suppose that $4a \equiv 4b \pmod{16}$? What is the most you can say about a and b?

   $a \equiv b \pmod 4$.

2. Suppose that $7a \equiv 7b \pmod{16}$? What is the most you can say about a and b?

   $a \equiv b \pmod{16}$.

3. A number $a \in \mathbb{Z}_m$ is called a *zero divisor* if there is some non-zero $b \in \mathbb{Z}_m$ such that $ab = 0$. Prove: if $a|m$ then a is a zero divisor in $\mathbb{Z}_m$.

   If $a|m$ then $ak = m$ for some k (with $0 < k < m$). So $k \neq 0$ in $\mathbb{Z}_m$ but $ak = 0$ in $\mathbb{Z}_m$.

4. Prove that if a is a zero divisor and b is any number, then ab is a zero divisor.

   There is some number c such that $ca = 0$, so $c(ab) = (ca)b = 0 \cdot b = 0$. Thus ab is a zero divisor if a is.

5. Prove that if there is some $d > 1$ such that $d|a$ and $d|m$, then a is a zero divisor in $\mathbb{Z}_m$.

   $a = dk$ for some k and $m = dj$ for some j, so $aj = dkj = (dj)k = mk = 0$.

6. A number $a \in \mathbb{Z}_m$ is called a *unit* if there is some $b \in \mathbb{Z}_m$ such that $ab = 1$. Prove: the product of two units is a unit.

   If a and b are units with $a^{-1}a = b^{-1}b = 1$, then $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1} \cdot 1 \cdot b = b^{-1}b = 1$, so ab is a unit.

7. Prove that no number can be both a unit and a zero divisor.

   Suppose that a is a unit, so that $1 = ab$ for some b. Then if $ca = 0$ for some c, multiplying both sides of $(1 = ab)$ gives $c = cab = 0 \cdot b = 0$, so $c = 0$. Thus if a is a unit then a cannot be a zero divisor.

8. (Harder) Prove that every number is $\mathbb{Z}_m$ is either a zero divisor or a unit.

   Easiest way: if $\gcd(a, m) = d > 1$ then a previous problem shows that a is a zero divisor in $\mathbb{Z}_m$. If $\gcd(a, m) = 1$ then Bezout's theorem says that there are some s, t such that $as + mt = 1$, so $as \equiv 1 \pmod m$, meaning that $a \cdot \overline{s} = 1$ in $\mathbb{Z}_m$ (where $\overline{s} = s \pmod m$)

9. What are the zero divisors in $\mathbb{Z}$? What are the units? What numbers are neither?

   0 is the only zero divisor. 1 and -1 are the only units.

10. For what values of m is every non-zero $a \in \mathbb{Z}_m$ a unit?

    This is the case if and only if m is a prime number, since $\gcd(a, p) = 1$ for any prime p and $0 < a < p$.