Chapters 4.1-4.2: Number Theory

Wednesday, September 16

Key Notes

- $a|b$ = a divides b = a is a divisor of b = b is divisible by a = $(\exists k \in \mathbb{Z})(ak = b)$
- $a \equiv b \pmod{m}$ if and only if $m|(b-a)$.
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.
- If $a|b$ and $a|c$ then $a|(mb + nc)$ for any $m, n \in \mathbb{Z}$.

Warmup

1. Today is Tuesday. What day will it be 1000 days from now?

   $1000 \pmod 7 = 300 \pmod 7 = 20 \pmod 7 = 6$, so 1000 days from now it will be Monday.

2. You are on a circular track 400 meters long. You run 3800 meters clockwise and 2200 meters counter-clockwise. How far are you from where you started?

   3800 - 2200 = 1600, which is divisible by 400. You ended up where you started.

3. Observations: If $30|n$ then $10|n$. If $25|n$ then $5|n$. If $18|n$ then $9|n$. Find a general rule.

   General rule: if $a|n$ and $b|a$ then $b|n$. Proof: There are j and k such that $aj = n$ and $bk = a$, so $b(kj) = aj = n$, meaning that $b|n$.

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 $2^{100} \pmod{10} = (2^4)^{25} \pmod{10} \equiv 6^25 \pmod{10} \equiv 6 \pmod{10}$, 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. $155 \cdot 822 \pmod{10}$

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

Divisibility

True or false? If true, prove. If false, find a counterexample.

1. $1|a$ for any a.

   True, since $1 \cdot a = a$ for any a.

2. $0|a$ for any a.

   False: let $a \neq 0$. Then for any k, $0 \cdot k = 0 \neq a$. This means that if $a \neq 0$, then $(\forall k)(0 \cdot k \neq a)$, which is the same as $\neg(\exists k)(0 \cdot k = a)$, or $0 \nmid a$.

3. $a|0$ for any a.

   True, since for any a, $a \cdot 0 = 0$.

4. If $a|b$ and $b|c$ then $a|c$.

   True. If $ak = b$ and $bj = c$, then $a(kj) = bj = c$.

5. If $a|b$ and $b|a$ then $a = b$.

   False: $a = 1$, $b = -1$.

6. If $a|c$ and $b|c$ then either $a|b$ or $b|a$.

   False: $a = 3, b = 5, c = 15$.

7. Suppose $a|b$. Then $a|(b + c)$ if and only if $a|c$.

   True: If $ak = b + c$ and $aj = b$ then $a(k - j) = c$.

   Conversely: if $an = c$ then $a(n + j) = b + c$.

8. If $2|n$ and $4|n$ then $8|n$.

   False: $n = 4$ and $n = -4$ are the only counterexamples.

Divisibility Tests

1. Prove that a number is divisible by 5 if and only if its last digit is 0 or 5.

   The key is to write the number n as $10t + u$, where u is the final digit and t is all of the other digits:

   $5|10t + u \Leftrightarrow 5|5(2t) + u \Leftrightarrow 5|u \Leftrightarrow u \in \{0, 5\}$.

2. Prove that a number is divisible by 4 if and only if its last two digits make a number divisible by 4.

   Similar answer to the previous problem:

   $4|100h + 10t + u \Leftrightarrow 4|4(25h) + 10t + u \Leftrightarrow 4|10t + u$.

3. Prove that for any integer n, either $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$.

   If $n = 2k$ is even then $n^2 = 4k^2$, and so $n \equiv 0 \pmod 4$.

   If $n \equiv \pm 1 \pmod 4$ then $n^2 \equiv 1 \pmod 4$.

4. Prove that 98765434 is not a perfect square.

   $98765434 \equiv 2 \pmod 4$, so by the previous problem it cannot be a perfect square.

5. Prove that 111111 cannot be written as the sum of any two square numbers (what are the possibilities for $a^2 + b^2 \pmod 4$?)

   Since any integer squared is 0 or 1 mod 4, the only options for the sum of two numbers are $0+0 = 0$, $1+0 = 1$, and 1+1=2. But $111111 \equiv 3 \pmod 4$.