Math 201 Class Discussion 31 October 2019

More on congruence

Fermat's Little Theorem

1. **Bezout's theorem**: For all integers, *a* and *b*, not both zero, there exist integers *x* and *y* such that ax + by = gcd(a, b). For example, gcd(24, 30) = (-1)24 + (1)30, gcd(7, 9) = (4)7 + (-3)9.
2. **Euclid's lemma**: If p is prime and p|ab then p|a or p|b.

   Proof: Suppose that $p\ is\ prime\ but\ not\ a\ divisor\ of\ a\ and\ that\ p|ab.$

   $We\ claim\ that\ p\ is\ a\ divisor\ of\ b.$

   Now gcd(p, a) = 1 (Why?)

   Bezout's theorem implies that $\exists x, y \in Z\ \ ax + py = 1.$

   Multiplying both sides by *b*: abx + bpy = b

   This implies that *p* is a divisor of *b*. (Why?)
3. Prove the more general version of Euclid's lemma: Same hypotheses except that *p* is assumed to be relatively prime to *a* (instead of requiring p to be prime). Same conclusion.
4. If $ca \equiv cb\ (mod\ n), must\ it\ follow\ that\ a\ \equiv b?$ (cancellation law?)
5. Suppose that *c* and *n* are relatively prime. Is the cancellation law valid?
6. Find the remainder when 7^{456} is divided by 8.
7. Find the remainder when 8^{2019} is divided by 9. Hint: consider 8^3.
8. Find the units digit of 3^{99}.
9. Find 17^{341} mod 5.
10. Find 2^{501} mod 17
11. Find 3^{701} mod 80.
12. Find 11^{23456} mod 5.
13. Find 13^{2345} mod 5.
14. **Fermat:** If *p* is a prime number, then for any integer *a*, the number $a^p - a$ is an integer multiple of *p*. In the notation of modular arithmetic, this is expressed as

    $a^p \equiv a$ (mod p). If *a* is not divisible by *p*, then $a^{p-1} \equiv 1$ (mod p).
15. Proof of Fermat: Consider a, 2a, 3a, … (p-1)a. Show that these p-1 numbers are distinct, non-zero, and thus must consist of {1, 2, .. p-1}. Multiply together. Then use cancellation rule.
16. Use Fermat's little theorem to show that 17 divides $11^{104}+1$.
17. If gcd(a, 35) = 1, show that $a^{12} \equiv 1\ (mod\ 35)$. Hint: Using Fermat, $a^6 \equiv 1\ (mod\ 7)\ and$ $a^4 \equiv 1\ (mod\ 5)$.
18. If gcd(a, 133) = gcd(b, 133) = 1, show that , for n ≥ 0, 133 is a divisor of $a^{18} - b^{18}$.
19. If gcd(a, 42) = 1, prove that 163 = (3)(7)(8) divides $a^6 - 1$.
20. Let a, b be integers. Then $a \equiv b\ (mod\ 6)\ if\ and\ only\ if\ a \equiv b\ (mod\ 2)\ and\ a \equiv b\ (mod\ 3)$
21. Find the units digit of 3^{100} by using Fermat.
22. Show that, for n ≥ 0, 13 is a divisor of $11^{12n+6} + 1$.

23. The three most recent appearances of Haley's comet were in the years 1835, 1910, and 1986. The next occurrence will be in 2061. Prove that
$1835^{1910} + 1986^{2061} \equiv 0 \ (mod\ 7)$.

24. Prove that $a^7 \equiv a \ (mod\ 42)$ for all n.

25. Prove that $a^{21} \equiv a \ (mod\ 15)$ for all n.

26. If gcd(a, 35) = 1, show that $a^{12} \equiv 1 \ (mod\ 35)$. Hint: Using Fermat, $a^6 \equiv 1 \ (mod\ 7)\ and$
$a^4 \equiv 1 \ (mod\ 5)$.

27. Let a, b be integers. Then $a \equiv b \ (mod\ 6)\ if\ and\ only\ if\ a \equiv b\ (mod\ 2)\ and\ a \equiv b\ (mod\ 3)$

28. Find the units digit of 3^{100}.