**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.

1. **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 $∃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?)

1. 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. {\displaystyle b=9}
2. If $ca≡cb \left(mod n\right), must it follow that a ≡b?$ (cancellation law?)
3. Suppose that *c* and *n* are relatively prime. Is the cancellation law valid?
4. Find the remainder when 7456 is divided by 8.
5. Find the remainder when 82019 is divided by 9. Hint: consider 83.
6. Find the units digit of 399.
7. Find 17341 mod 5.
8. Find 2501 mod 17
9. Find 3701 mod 80.
10. Find 1123456 mod 5.
11. Find 132345 mod 5.
12. **Fermat:** If *p* is a prime number, then for any [integer](https://en.wikipedia.org/wiki/Integer) *a*, the number *ap* - *a* is an integer multiple of *p*. In the notation of [modular arithmetic](https://en.wikipedia.org/wiki/Modular_arithmetic), this is expressed as

$a^{p}≡a$ (mod p). If *a* is not divisible by *p*, then $a^{p-1}≡1$ (mod p). {\displaystyle a^{p}\equiv a{\pmod {p}}.}

1. 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.
2. Use Fermat’s little theorem to show that 17 divides 11104+1.
3. If gcd(a, 35) = 1, show that a12 $≡1 \left(mod 35\right).$ Hint: Using Fermat, $a^{6}≡1 \left(mod 7\right) and $

$a^{4}≡1 \left(mod 5\right)$.

1. If gcd(a, 133) = gcd(b, 133) = 1, show that , for n ≥ 0, 133 is a divisor of a18 – b18.
2. If gcd(a, 42) = 1, prove that 163 = (3)(7)(8) divides a6 – 1.
3. Let a, b be integers. Then $a≡b \left(mod 6\right) if and only if a≡b \left(mod 2\right) and a≡b (mod 3)$
4. Find the units digit of 3100 by using Fermat.
5. Show that, for n ≥ 0, 13 is a divisor of 1112n+6 + 1.
6. 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

18351910 + 19862061 $≡0 \left(mod 7\right).$

1. Prove that a7 $≡a \left(mod 42\right)$ for all n.
2. Prove that a21 $≡a \left(mod 15\right)$ for all n.
3. If gcd(a, 35) = 1, show that a12 $≡1 \left(mod 35\right).$ Hint: Using Fermat, $a^{6}≡1 \left(mod 7\right) and $

$a^{4}≡1 \left(mod 5\right)$.

1. Let a, b be integers. Then $a≡b \left(mod 6\right) if and only if a≡b \left(mod 2\right) and a≡b (mod 3)$
2. Find the units digit of 3100.