FM2 Assignment #38 Name: Jerry Jiang

1. An arithmetic sequence has first term 2 and common difference 4. Another arithmetic sequence has first term 7 and common difference 5. Find the set of numbers which are members of both sequences.

   By inspection, the first positive integer that satisfies this is 22. lcm(4,5)=20, so the set of numbers are the arithmetic sequence with first term 22 and common difference 20.

反馈
2. That works!
3. Should explain why a\neq a^{-1}. [1.5]
5. This was also my approach.

Excellent!
分数
9.5 / 10

2. What is the remainder when 314^{164} is divided by 165? Make sure to justify your answer.

   To use Fermat's little theorem, p has to be a prime while 165 is not.
   Let's apply Euler's theorem as gcd(165,314)=1. Phi(165)=(3−1)(5−1)(11−1)=80.
   So 314^(80)≡1 mod 165. 314^(164)=314^(80*2+4)=(314^(80)^2)*314^(4)≡1*(−16)^(4)=65536≡31 mod 165.
   Hence the remainder is 31.
   I wasn't able to be live in the last class, but from the recording, I think you didn't talk about Euler's theorem. What's the method you want us use to solve it?

3. Show that every cyclic group of order greater than two has at least two generators.

   If the group is cyclic and it has more than two elements, then it at least have one generator which can generate the group. The other generator is its inverse, which produces the group in the reversed direction.

4. (a) Show that $a_n \times 10^n + a_{n-1} \times 10^{n-1} + \cdots + a_1 \times 10 + a_0 \equiv a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^n a_n \pmod{11}$.

Suppose n is an even number. 10^(2k)≡1 mod 11, 10^(2k+1)≡−1 mod 11. So we can say (a_n)−(a_n−1)+(a_n−2)−(a_n−3)+……−(a_1)+(a_0)≡the original number mod 11, which is what we want. The result is still consistent when n is odd. This is the rule of divisibility by 11.

(b) Alice claims 27 182 818 284 590 452 is divisible by 11. Bob disagrees. Who is right? Explain.

2−7+1−8+2−8+1−8+2−8+4−5+9−0+4−5+2=−22≡0 mod 11. Alice is right.

5. If p and q are distinct primes, prove that $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

p^(q−1)≡1 mod q, q^(p−1)≡0 mod q. Adding them up and we get: p^(q−1)+q^(p−1)≡1 mod q. Similarly we get: p^(q−1)+q^(p−1)≡1 mod p. So both p and q divides p^(q−1)+q^(p−1)−1. gcd(p,q)=1, so pq divides p^(q−1)+q^(p−1)−1, which is the same as p^(q−1)+q^(p−1)≡1 mod pq. Is there another way of doing this?