CS 70 Discrete Mathematics and Probability Theory
Summer 2016 Psmoas, Dinh and Ye Discussion 4A

1. Baby Fermat

Assume that a does have a multiplicative inverse $\pmod m$. Let us prove that its multiplicative inverse can be written as $a^k \pmod m$ for some $k \geq 0$.

- Consider the sequence $a, a^2, a^3, \ldots \pmod m$. Prove that this sequence has repetitions.
- Assuming that $a^i \equiv a^j \pmod m$, where $i > j$, what can you say about $a^{i-j} \pmod m$?
- Prove that the multiplicative inverse can be written as $a^k \pmod m$. What is k in terms of i and j?

2. Product of Two

Suppose that $p > 2$ is a prime number and S is a set of numbers between 1 and $p-1$ such that $|S| > \frac{p}{2}$. Prove that any number $1 \leq x \leq p-1$ can be written as the product of two (not necessarily distinct) numbers in S, mod p.

3. RSA

In this problem you play the role of Amazon, who wants to use RSA to be able to receive messages securely.

1. Amazon first generates two large primes p and q. She picks $p = 13$ and $q = 19$ (in reality these should be 512-bit numbers). She then computes $N = pq$. Amazon chooses e from $e = 37, 38, 39$. Only one of those values is legitimate, which one? (N, e) is then the public key.
2. Amazon generates her private key d. She keeps d as a secret. Find d. Explain your calculation.

```
e-gcd(216,37)
  e-gcd(37,31)
    e-gcd(31,6)
      e-gcd(6,1)
        e-gcd(1, 0)
        return (1,1,0)
      return (1,0,1)
    return (1,1,-5)
```

```
    return (1,-5,6)
  return (1,6,-35)
```

3. Bob wants to send Amazon the message $x = 102$. How does he encrypt his message using the public key, and what is the result?
   Note: For this problem you may find the following trick of fast exponentiation useful. To compute x^k, first write k in base 2 then use repeated squaring to compute each power of 2. For example, $x^7 = x^{4+2+1} = x^4 \cdot x^2 \cdot x^1$.
4. Amazon receives an encrypted message $y = 141$ from Charlie. What is the unencrypted message that Charlie sent her?