CS 70 Discrete Mathematics and Probability Theory
Fall 2016 Seshia and Walrand

Discussion 5A

1. **Bijections** Consider the function

$$f(x) = \begin{cases} x, & \text{if } x \geq 1; \\ 3x-2, & \text{if } \frac{1}{2} \leq x < 1; \\ -x, & \text{if } -1 \leq x < \frac{1}{2}; \\ 2x+3, & \text{if } x < -1. \end{cases}$$

(a) If the domain and range of f are $\mathbb{N}$, is f injective (one-to-one), surjective (onto), bijective?

Solution: Yes, Yes, Yes.

(b) If the domain and range of f are $\mathbb{Z}$, is f injective (one-to-one), surjective (onto), bijective?

Solution: No, No, No.

(c) If the domain and range of f are $\mathbb{R}$, is f injective (one-to-one), surjective (onto), bijective?

Solution: No, Yes, No.

2. **Amazon RSA**

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

(a) 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.

Solution: Since 38 and 39 are not relatively prime to $p-1 = 12$ and $q-1 = 18$, they cannot be inverted mod $(p-1)\cdot(q-1) = 216$, so a decryption key cannot be obtained for them. Thus, only $e = 37$ works. The public key then is $(N, e) = (247, 37)$.

(b) Amazon generates her private key d. She keeps d as a secret. Find d. Explain your calculation.

Solution: We compute $d \equiv e^{-1} \equiv 37^{-1} \pmod{216}$.

```
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)
```

Solution: Thus $d \equiv -35 \equiv 181 \pmod{216}$.

(c) 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, $x^7 = x^{4+2+1} = x^4 \cdot x^2 \cdot x^1$.

Solution: The encrypted message is $y \equiv x^e \equiv 102^{37} \pmod{247}$. Using fast exponentiation, we compute:

$$\begin{aligned} 102^2 &\equiv 30 \pmod{247} \\ 102^4 \equiv 30^2 &\equiv 159 \pmod{247} \\ 102^8 \equiv 159^2 &\equiv 87 \pmod{247} \\ 102^{16} \equiv 87^2 &\equiv 159 \pmod{247} \\ 102^{32} \equiv 159^2 &\equiv 87 \pmod{247} \end{aligned}$$

Then, $y \equiv 102^{37} \equiv 102^{32} \cdot 102^4 \cdot 102 \equiv 102 \pmod{247}$. Notice that the encrypted message is the same as the original!

(d) Amazon receives an encrypted message $y = 141$ from Charlie. What is the unencrypted message that Charlie sent her?

Solution: We decrypt the message by raising to the dth power: $x \equiv y^d \equiv 141^{181} \pmod{247}$. We compute the powers:

$$\begin{aligned} 141^2 &\equiv 121 \pmod{247} \\ 141^4 \equiv 121^2 &\equiv 68 \pmod{247} \\ 141^8 \equiv 68^2 &\equiv 178 \pmod{247} \\ 141^{16} \equiv 178^2 &\equiv 68 \pmod{247} \\ 141^{32} \equiv 68^2 &\equiv 178 \pmod{247} \\ 141^{64} \equiv 178^2 &\equiv 68 \pmod{247} \\ 141^{128} \equiv 68^2 &\equiv 178 \pmod{247} \end{aligned}$$

Then $x \equiv 141^{181} \equiv 141^{128} \cdot 141^{32} \cdot 141^{16} \cdot 141^4 \cdot 141 \equiv 141 \pmod{247}$.
By now, you may have guessed that $\forall x \in \{0, \ldots, 246\}$, $x^{37} \equiv x \pmod{247}$. We can prove this by noting that $e = 37 \equiv 1 \pmod{p-1}$ and $e = 37 \equiv 1 \pmod{q-1}$. Thus,

$e = 1 + j(p-1) = 1 + k(q-1)$ for some j and k. By Fermat's little theorem, $x^{e-1} = x^{j(p-1)} \equiv 1 \pmod{p}$ and $x^{e-1} = x^{k(q-1)} \equiv 1 \pmod{q}$ where x is coprime with p and q. Then by the Chinese remainder theorem, $x^{e-1} \equiv 1 \pmod{pq}$, so $x^e \equiv x \pmod{pq}$. Though we omit it here, we can also show that $x^e \equiv x \pmod{pq}$ when x is not coprime with p and q. See the very similar RSA proof for details.

Moral of the story: stick with $e = 3$!

3. **RSA Reasoning** In RSA, if Alice wants to send a confidential message to

   Bob, she uses Bob's public key to encode it. Then, Bob uses his

   private key to decode the message. Suppose that Bob chose $N = 77$ and $e = 3$, so his public key is $(3, 77)$. Bob chose $d = 26$, so his private key is $(26, 77)$.

   Will this work for encoding and decoding messages? If not, where did

   Bob first go wrong in the above sequence of steps and what is the

   consequence of that error? If it does work, show that it works.

   Solution: e should be co-prime to $(p-1)(q-1)$.
   Since $e = 3$ is not co-prime to $(7-1)(11-1) = 60$, this is incorrect. Consequently, e does not have a multiplicative inverse mod 60.

4. **RSA with Multiple Keys** Members of a secret society know a secret word. They transmit this secret word x between each other many times, each time encrypting it with the RSA method. Eve, who is listening to all of their communications, notices that in all of the public keys they use, the exponent e is the same. Therefore the public keys used look like $(e, N_1), \ldots, (e, N_k)$ where no two N_i's are the same. Assume that the message is x such that $0 \leq x < N_i$ for every i.

   (a) Suppose Eve sees the public keys $(7, 35)$ and $(7, 77)$ as well as the corresponding transmissions. How can Eve use this knowledge to break the encryption?

   Solution: Yes. Note that gcd(77, 35) = 7. She can figure out the gcd of the two numbers using the gcd algorithm, and then divide 35 by 7, getting 5. Then she knows that the p and q corresponding to the first transmission are 7 and 5, and can break the encryption.

   (b) The secret society has wised up to Eve and changed their choices of N, in addition to changing their word x. Now, Eve sees keys $(3, 5 \times 23)$, $(3, 11 \times 17)$, and $(3, 29 \times 41)$ along with their transmissions. Argue why Eve cannot break the encryption in the same way as above.

   Solution: Since none of the N's have common factors, she cannot find a gcd to divide out of any of the N's. Hence the approach above does not work.