Worksheet 5: Cryptography

1. Compute 2^{222} mod 101.

2. Our goal is to come up with a *code* modulo 101; that is, we want to send a message consisting of 2-digit numbers, and we'd like to encode it in such a way that only our friends can decode it. The first coding scheme we'll describe is due to Diffie and Hellman. It is a *public-key code* because part of the code is known to everyone. Here's how it works: you and your friend choose a prime number p (such as 101) and an integer g between 2 and $p-1$. Both of these numbers are public (so, e.g., you two can safely discuss these numbers on the phone or over the internet—if someone wiretaps you, no problem). Now you *secretly* choose an integer m, and your friend *secretly* chooses an integer n. You compute $g^m \bmod p$ and tell your friend the result. Your friend computes $g^n \bmod p$ and tells you the result. The secret key that you both can use is

$$s \equiv g^{mn} \equiv (g^m)^n \equiv (g^n)^m \bmod p\,.$$

The last two equalities explain why both you and your friend can easily compute s. You can now use s to encode messages, e.g., using multiplication mod p, and s^{-1} to decode. Can you see why it's hard to compute s if you know p, g, g^m, and g^n? How could you make this cryptosystem safer? Do you see a way to "break" it?

3. Our second coding scheme is the *RSA cryptosystem*.[1] Here's how it works: You need two prime numbers p and q, compute their product $m = pq$, find a number b that is relatively prime to $\phi(m) = (p-1)(q-1)$, and compute an inverse c of b modulo $\phi(m)$, i.e., $bc \equiv 1 \bmod \phi(m)$. You keep all of this private except for the numbers m and b which you make public (in particular, your friends know m and b). To send you a message d, your friend encodes it as

$$e = d^b \bmod m\,.$$

You can decode your friend's message by computing

$$d = e^c \bmod m\,.$$

Explain why this decoding works. What makes this cryptosystem safe? How could you make it safer? What would one need to break it?

4. Stein 2.10, 2.30, 3.4, 3.5.

5. Write down a precise statement for each definition we have given this week. For each definition, give an example and a non-example.

[1] The RSA cryptosystem is named after its discoverers Ron Rivest, Adi Shamir, and Leonard Adleman.