M328K – Rusin – HW8 – Due Thursday, May 4, 2017

1. (a) Compute $\mathrm{ord}_{35}(9)$, i.e. the order of 9 modulo 35.

(b) Show that if p and q are distinct primes then for all a,

$$\mathrm{ord}_{pq}(a) = \mathrm{lcm}(\mathrm{ord}_p(a), \mathrm{ord}_q(a))$$

2. Find all primitive roots modulo 18.

3. The number $a = 2$ is a primitive root for $p = 11$ and also for $p = 13$. (You don't have to prove this.)

(a). For each of these two primes p, write -1 as a power of 2 (mod p). Can you make a corresponding statement for general primes p?

(b). Use this information to decide whether the congruence $x^2 \equiv -1$ is solvable for either of these primes. Can you decide for a general prime p whether or not -1 is a square mod p?

4. (a) Solve these two equations for x and y in terms of s and t:

$$x + y = s \qquad\qquad x \cdot y = t$$

(b) The number $N = 89077$ is the product of two primes and has $\phi(N) = 88480$. Find the prime factorization of N. (Hint: if $N = pq$ then $\phi(N) = (p-1)(q-1)$ so you can figure out both the sum and the product of the two primes. So use part (a) and a calculator.)

5. Here's a recap of our encryption protocol: Bob publicly announces his modulus N and his encryption exponent d and invites people like Alice to send him a message x by first encrypting it, sending Bob the number $y = x^d$ (mod N) instead of sending him x itself. Bob can decode the messages by computing $x = y^e$ (mod N), where e is the inverse of d modulo $\phi(N)$. (Of course Bob has to know $\phi(N)$ to do this, so in order to choose N he picked two big primes first, and let N be their product.) He can allow N, d, and y to be known to all the public as long as N is too hard for anyone else to factor.

For the sake of definiteness let's suppose Bob picks $d = 11$ and $N =$

$$8539734222673567065463550870400829907215612005311510800855247$$

(a product of two primes that Bob likes) and announces these numbers to the public. (Don't worry, I won't make you do anything with N yourself!)

This system is believed to be pretty secure. But the point of this exercise is to show that tiny mistakes in judgment can render it insecure.

Suppose Bob's brother Charlie also wants to receive secret messages. For simplicity they decide Charlie will use the same N as Bob, but Charlie announces a different encryption exponent d', say $d' = 27$. (Bob shares his knowledge of $\phi(N)$ with Charlie so they can both compute their different decryption exponents. This means each could decrypt messages which are intended for his brother, but that's not a problem — they trust each other completely.)

OK, so Alice has a secret message x she wants to send to both brothers. Following the protocol she computes $y_B = x^d \pmod N$ and tapes this number y_B on Bob's door because, hey, this is a secure protocol, right? Then she computes $y_C = x^{d'}$ and similarly tapes that to Charlie's door. Each of Bob and Charlie proceeds to decode the message he received. (Remember, it's the same message x sent to both.)

Meanwhile, Eve knows the brothers' modulus N, but is unable to factor it. She knows the encryption exponents $d = 11$ and $d' = 27$. She can read y_B but cannot compute x from that. She can read y_C too and wouldn't be able to compute x from it either — if that were all she knew. However, since she knows *both* y_B and y_C she manages to decode the message x! How did she do that?

(Hint: $5 \cdot 11 - 2 \cdot 27 = 1$.)