M328K – Rusin – HW8 ANSWERS

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

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

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

ANSWER: Let $k = \text{ord}_p(a)$ and let $\ell = \text{ord}_q(a)$. Then $a^n \equiv 1 \pmod{p}$ iff n is a multiple of k; similarly $a^n \equiv 1 \pmod{q}$ iff n is a multiple of ℓ. Thus $a^n \equiv 1 \pmod{pq}$ iff both events hold, i.e. iff n is a multiple of both k and ℓ. The smallest such n is then $\text{lcm}(k, \ell)$ by definition of what "lcm" means!

(This gives part (a) as a corollary but it's also an illustration: $9^n \equiv 1 \bmod 5$ iff n is even, and it's congruent to 1 mod 7 iff n is a multiple of 3, so it's congruent to 1 mod 35 iff n is an even multiple of 3, i.e. a multiple of 6.)

2. Find all primitive roots modulo 18.

ANSWER: The six invertible classes mod 18 are $\{1, 5, 7, 11, 13, 17\}$. Then we can check that $5^2 \equiv 7$ and $7^2 \equiv 13$ are squares, so they cannot be primitive roots, and of course 1 and -1 are cubes and so they are not primitive roots either. This leaves just 5 and $11 = 5^{-1}$ which are both primitive roots.

This reasoning applies in general: you want to avoid all the pth powers for each prime $p|\phi(n)$. The remaining classes are the primitive roots. If r is one of the primitive roots, all the others are (of course) expressible as power r^k of r, but avoiding pth powers means that this k can not be a multiple of any of the primes dividing $\phi(n)$. In other words, once you find one primitive root r, the others are of the form r^k where k is one of the integers which is invertible modulo $\phi(n)$ (i.e. k is an element of $\mathbf{Z}^\times_{\phi(n)}$). There are $\phi(\phi(n))$ such candidates k, meaning there are $\phi(\phi(n))$ primitive roots. The case $n = 18$ is meant to be an illustration of this.

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?

ANSWER: If p is any prime and r is any primitive root for p, then let $x = r^{(p-1)/2}$. This has the feature that $x^2 = r^{(p-1)} \equiv 1 \bmod p$ by Euler's theorem. But we know the only solutions to $x^2 \equiv 1$ are $x = 1$ and $x = -1$, as long as the modulus is prime. On the other hand x cannot equal 1: the fact that r is a primitive root means that the *least* exponent on r that will give $r^k \equiv 1$ is $k = \phi(p)$, so that $r^{(p-1)/2} \equiv 1$ is impossible. Hence $r^{(p-1)/2} \equiv -1$. In particular, $-1 \equiv 2^5 \bmod 11$ and $-1 \equiv 2^6 \bmod 13$.

When $p = 13$ or indeed any prime that's congruent to 1 modulo 4, it follows that $(p-1)/2$ is even. Hence this x is a square. (It's the square of $r^{(p-1)/4}$!) But we just established that $x = -1$, so -1 is a square for such primes.

Conversely if -1 is a square mod p, let y be one of its square roots, and write this y as a power of r, say $-1 \equiv r^k$. Then we have written (-1) as both $r^{(p-1)/2}$ and as $y^2 = r^{2k}$. Since r is a primitive root this requires $(p-1)/2 \equiv 2k \bmod \phi(p) = p-1$. Since both $2k$ and $p-1$ are even, so must $(p-1)/2$ be, which means $p \equiv 1 \bmod 4$. In particular, -1 is not a square modulo 13.

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.)

ANSWER: For (a), observe that x and y are the roots of the polynomial $(X-x)(X-y) = X^2 - sX + t$. We may express this using the quadratic formula if we like: x and y must be the two values of

$$(s \pm \sqrt{s^2 - 4t})/2$$

If a number N is known to be the product of two distinct primes, i.e. $N = pq$, then $\phi(N) = (p-1)(q-1) = pq - (p+q) + 1 = N - (p+q) + 1$. Thus

$$pq = N \qquad (p+q) = N + 1 - \phi(N)$$

From part (a) we can then write a formula which produces p and q from N and $\phi(N)$. For example, in the case given, we deicde $\{p, q\} = \{281, 317\}$.

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 $y = x^d \pmod N$ instead of sending him x itself. Bob can decode the messages by computing $x = y^e \pmod N$, 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 $N =$

$$85397342226735670654635508704008299072156120053115108008552 47$$

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

ANSWER: Eve had only to perform some computations modulo N: $(y_B)^5 \cdot (y_C)^{-2} \equiv (x^{11})^5 \cdot (x^{27})^{-2} \equiv x^{5 \cdot 11 - 2 \cdot 27} = x^1 = x$ so Eve can recover the original plaintext from the two ciphertexts!

There is no way to predict how clever Eve will be so it is best to avoid any kind of overlap of data! You should not share your N even with someone who is completely trustworthy!

By the way, $N = 31415926535897932384626433383457 \times 27182818284590452353602874714 71$. $\blacksquare$
Perhaps you recognize some of those digits?