Math 261 — Fall 2022
Number Theory
`https://sites.aub.edu.lb/kmakdisi/`
Problem set 4, due Friday, September 30 at the beginning of class

Exercise 4.1: a) Find $\phi(101)$, $\phi(6561)$, and $\phi(25200)$.

b) Compute the remainder of 2^{705} when divided by 101, and the remainder of 11^{17282} when divided by 25200.

Exercise 4.2: a) Use the Chinese Remainder Theorem to find all the solutions of the equation $x^2 \equiv 1 \pmod{1729}$. (Find the factorization of 1729 first.)

b) Show that for all $a \in \mathbf{Z}$ with $\gcd(a, 1729) = 1$, we have $a^{1728} \equiv 1 \pmod{1729}$. This holds even though 1729 is not prime; one says that 1729 is a **Carmichael** number.

c) Find a smaller k (i.e., $1 < k < 1728$) such that for all $a \in \mathbf{Z}$ with $\gcd(a, 1729) = 1$, we have $a^k \equiv 1 \pmod{1729}$. Make k as small as possible.

Exercise 4.3: Let p be a prime.

a) Show that $\overline{1+p}$ has multiplicative order p in $(\mathbf{Z}/p^2\mathbf{Z})^*$. Conclude that for $k \geq 2$, the multiplicative order of $\overline{1+p}$ in $(\mathbf{Z}/p^k\mathbf{Z})^*$ is a multiple of p. (Challenge: prove that this order is in fact a *power* of p.)

b) Conclude that if $p^2|N$, then there exists $\overline{a} \in (\mathbf{Z}/N\mathbf{Z})^*$ whose multiplicative order in $(\mathbf{Z}/N\mathbf{Z})^*$ is a multiple of p. (Caution: $1 + p$ might not be relatively prime to N. I suggest that you write $N = p^k M$, where $k \geq 2$ and $p \nmid M$, and choose a by choosing $a \bmod p^k$ and $a \bmod M$ separately and invoking the Chinese Remainder Theorem.)

c) Deduce that N is not a Carmichael number. (N.B., this shows that if N is a Carmichael number, then it is squarefree, i.e., it is the product of distinct prime numbers.)

Exercise 4.4: a) Factor $N = 144869$ and find $L = \phi(144869)$.

b) Consider the map $f : (\mathbf{Z}/144869\mathbf{Z})^* \to (\mathbf{Z}/144869\mathbf{Z})^*$ given by $f(\overline{x}) = \overline{x}^{103}$. Show that f is a bijection by finding an inverse map of the form $g(\overline{y}) = \overline{y}^e$ for some e that you must find. (Hint: e is determined by a certain equation mod L.)

c) Solve for $\overline{x} \in (\mathbf{Z}/144869\mathbf{Z})^*$ that satisfies the equation $\overline{x}^{103} = \overline{12}$. You will probably need to use the repeated squaring algorithm — look it up! — for quickly computing powers mod 144869.

d) How many $\overline{x} \in (\mathbf{Z}/144869\mathbf{Z})^*$ satisfy $\overline{x}^{144868} = \overline{1}$? What does this say about the probability of finding a "false positive" to the Fermat test for primality?

Cultural note for (a–c): if N is very large, and one does not know the factorization of N, then it is believed that it is difficult to find L and e; so the map f is an "encryption" map that (we hope) can be only "decrypted" (i.e., inverted) by the person who chose large primes p, q and published only their product N and the number $d = 103$. This is the basis of the RSA cryptographic system, which you should look up in Section 8.8 of Davenport.

Exercise 4.5: Fix $n > 0$.

a) If $d > 0$ and $d|n$, show that the number of elements $\overline{a}$ in $\mathbf{Z}/n\mathbf{Z}$ such that $\gcd(a, n) = d$ is equal to $\phi(n/d)$.

Hint: write $a = da'$ and $n = dn'$. As an example of what you need to prove, the number of elements $\overline{a}$ in $\mathbf{Z}/15\mathbf{Z}$ with $\gcd(a, 15) = 3$ is exactly $\phi(5) = 4$: the values of $\overline{a}$ are $\overline{3}, \overline{6}, \overline{9}, \overline{12}$.

b) Show that $n = \sum_{d|n} \phi(n/d)$, and deduce that $n = \sum_{d|n} \phi(d)$. Hint for the first part: separate the elements in $\mathbf{Z}/n\mathbf{Z}$ according to their GCD with n.

c) Show that the equations in part (b) allow one to compute $\phi(n)$ recursively by writing the equations for all n' with $n'|n$. For example, if $n = 15$, one can combine the results for all $n' \in \{1, 3, 5, 15\}$ to get $1 = \phi(1)$; $3 = \phi(1)+\phi(3)$; $5 = \phi(1)+\phi(5)$; and $15 = \phi(1)+\phi(3)+\phi(5)+\phi(15)$. This uniquely determines (in order) the numbers $\phi(1), \phi(3), \phi(5), \phi(15)$.

Exercise 4.6 (optional, for extra credit): Look up the Moebius inversion formula, and combine it with the results of Exercise 4.5 to deduce that

$$\phi(n) = n \prod_{p|n,\, p \text{ prime}} \Big(1 - \frac{1}{p}\Big).$$