Homework 6

Sean Eva

April 2022

1. (a) $\mu(12) = \mu(2*2*3) = 0$
   (b) $\mu(15) = \mu(3*5) = (-1)^2 = 1$
   (c) $\mu(30) = \mu(2*3*5) = (-1)^3 = -1$
   (d) $\mu(50) = \mu(2*5*5) = 0$
   (e) $\mu(1001) = \mu(7*11*13) = (-1)^3 = -1$
   (f) $\mu(2*3*5*7*11*13) = (-1)^6 = 1$
   (g) $\mu(10!) = \mu(10*9*8*7*6*5*4*3*2) = \mu(2*5*9*8*7*6*5*4*3*2) = 0$

11. *Proof.* Consider two nonnegative integers $n = 36k+8$ and $n+1 = 36k+9$. n is divisible by 4 which implies that it has a square of 2 in the set of its factors and the second number, $n+1$ is divisible by 9 which implies that it has a square of 3 in its factors. Since both of these numbers contain squares in their prime factorizations, then their Mobius Function evaluations are 0. This $\mu(n)+\mu(n+1) = \mu(36k+8)+\mu(36k+9) = 0+0 = 0$. Therefore, there are infinitely many consecutive positive integers such that their summation of their Mobius Function evaluations are 0. $\square$

15. *Proof.* Consider an identity function $h(n) = n$. Then if n is a positive integer, then $n = \sum \phi(d)$. Therefore, $h(n) = n = \sum \phi(d)$. Now using Mobius inversion formula we get $\phi(n) = \sum \mu(d)h(n/d) = \sum \mu(d)(n/d) = n \sum \mu(d)d$. Therefore, if n is a positive integer, then $\phi(n) = n \sum \mu(d)/d$. $\square$

17. *Proof.* Consider a multiplicative function f with $f(1) = 1$. If F is multiplicative, then f is also multiplicative. Thus, both f and μ are also multiplicative. Now. as f and μ are multiplicative, then their product μf is also multiplicative. Similarly, the summation $\sum \mu(d)f(d)$ is also multiplicative. Therefore, $\sum \mu(d)f(d) = \mu(p^a)f(p^a) + \mu(p^{a-1})f(p^{a-1}) + ... + \mu(p)f(p) + \mu(1)f(1)$. According to the definition, for exponents greater than 1, the value of $\mu(p^i) = 0$. Therefore, we can simplify this to be $\sum \mu(d)f(d) = \mu(p)f(p) + \mu(1)f(1) = 1 - f(p)$. Now, as $n = p_1^{a_1}p_2^{a_2}...p_k^{a_k}$ we get that $\sum \mu(d)f(d) = (1-f(p_1))(1-f(p_2))...(1-f(p_k))$. $\square$

23. *Proof.* Consider the identity given by $\sum \mu(d)f(d) = (1-f(p_1))(1-f(p_2))...(1-f(p_k))$ where f is a multiplicative function with $f(1) = 1$. And $n = p_1^{a_1}p_2^{a_2}...p_k^{a_k}$ as a prime factorization. We are able to write $\sum \mu^2(d)$ in the form of the identity stated above because it can be considered $f(d) = \mu(d)$ and also $\mu(1) = 1$. Therefore, $\sum \mu^2(d) = (1-\mu(p_1))(1-\mu(p_2))...(1-\mu(p_k))$ for primes p_i. Since $\mu(p) = -1$ for prime p we know that $\sum \mu^2(d) = (1-(-1))(1-(-1))...(1-(-1)) = 2*2*...*2 = 2^k$. Therefore, we know that $\sum \mu^2(d) = 2^k$ where k is the number of distinct prime factors of d. $\square$

4. NPWJE APNSP QESW

38. If we let $p_1p_2...p_m$ and $q_1q_2...q_m$ be two different plain text streams. If $k_1k_2...k_m$ be the keystream used to encrypt the two plain texts $E_{k_i}(p_i) = k_i + p_i(\mod 2)$ and $E_{k_i}(q_i) = k_i + q_i(\mod 2)$ and the corresponding ciphertext streams are $E_{k_i}(p_i) + E_{k_i}(q_i) = k_i + p_i + k_i + q_i(\mod 2) = 2k_i + p_i + q_i(\mod 2) = p_i + q_i(\mod 2)$. It can then also be shown that if someone can encrypt a bit string and have access to the resulting cipher string, the key string can be found. If we have a key of 0 then the cipher text would be the same as the plain text and we would know that the key is 0. Similarly, if the key is 1 then we would know this because the cipher text would be different from the plain text.

1. $p = 97, q = 151$

3. It is known that $P \leq n$. If $(P, n) \neq 1$, then there must be greatest common divisors of P and n must be one of factors of n that is p or q. $(P, n) = p$ or $(P, n) = q$. Now, using the Euclidean algorithm to find the greatest common factors of (P, n), the Euclidean Algorithm will give us one of the factors of n and divide n by this calculated factor to get another factor. Therefore, if plaintext P is not relatively prime to the enciphering modulus, then the cryptanalyst can factor n.

4. For any integer n, there are n integers up to and including n. Now consider the given $n = pq$. Therefore, the following are the integers that are no relatively prime to n : $p, 2p, 3p, ..., qp; q, 2q, 3q, ..., (p-1)q$. Therefore, there are $q + p - 1$ integers up to n that are not relatively prime to n. This is also the number of ways the interested event is expected to occur. Therefore, the required probability is $\frac{q+p-1}{n} = \frac{q}{n} + \frac{p}{n} - \frac{1}{n} = \frac{q}{pq} + \frac{p}{pq} - \frac{1}{pq} = \frac{1}{p} + \frac{1}{q} - \frac{1}{pq}$.

12. Fermat's Factorization method hints that an odd number can be written as a difference of two squares that when factored as $a^2 - b^2 = (a+b)(a-b)$. If the primes are close together, then b will be a small number that will be easily found even under guess and check and even faster using a computer based algorithm.

13. Consider a plaintext P. Now consider two exponents e_1, e_2. If we have $(e_1, e_2) = a$ then there are some x, y such that $a = xe_1 + ye_2$. The encryption of the first part is given as $C_1 = p^{e_1} (\mod n)$ and the second part is $C_2 = P^{e_2} (\mod n)$ where C_1, C_2 are the cipher texts. Now, since we now know C_1, C_2, e_1, e_2 we are able to easily compute x, y as $C_1^x, C_2^y = P^{e_1 x} P^{e_2 y} = P^{e_1 x + e_2 y} = P^a (\mod n)$. If a is relatively small, then it may not be difficult to computer the $a^t h$ root of P^a and thereby to recover P.

14. Let us say the three modules are pairwise, relatively prime. We can use the Chinese remainder theorem to solve the system of congruences and give us a least non-negative integer $x = p^3 (\mod (n_1, n_2, n_3)$. By construction $p < x_i$ for $i = 1, 2, 3$, we will have $p^3 < x_1, x_2, x_3$. It is guaranteed by the theorem that x must be a perfect cube whose cube root is easily computable. And this will be a plaintext $= p$.

12. The objective is to show that if the integers $'a'$ and $'b'$ are relatively prime and $(\text{ord}_n a, \text{ord}_n b) = 1$ then $\text{ord}_n ab = \text{ord}_n a \text{ord}_n b$. As the integers a and b are prime integers, therefore $(a, n) = 1, (b, n) = 1$ which implies that $(\text{ord}_n a, \text{ord}_n) = 1$. Now consider that $\text{ord}_n a = k_1$ and $\text{ord}_n b = k_2$. Therefore, $a^{k_1} \equiv 1(\mod n)$ and $a^{k_2} \equiv 1(\mod n)$ implies that $a^{k_1 k_2} \equiv 1(\mod n), b^{k_1 k_2} \equiv 1(\mod n)$. Now, if we multiply both of these equations we get that $(ab)^{k_1 k_2} \equiv 1(\mod n)$ which means that $\text{ord}_n ab = k_1 k_2$. Therefore, it is clear that from the above that $\text{ord} ab = \text{ord} a \text{ord} b$ as desired.

16. From Euler's Theorem we have that for a positive integer a relatively prime to another integer n, $a^{\phi(n)} \equiv 1(\mod n)$. Therefore, for a positive integer m a prime number we can write that, $a^{m-1} \equiv 1(\mod m)$. We also know that $\text{ord}_m a | \phi(m)$. Therefore, if $\text{ord}_m a = m - 1$ then it must divide $\phi(m)$. We also know that $\phi(m) \leq m - 1$. Therefore, $\phi(m) = m - 1$, which implies finally that the positive integer m must be a prime.

12. Let p be a prime and let r be a primitive root of p. Then the inverse $r^{-1} = r^{p-2}$ is a primitive root as well. Thus, we can group the primitive roots in pairs of mutually inverse roots whenever r and r^{-1} are different from each other. If we investigate when r and r^{-1} can coincide we get that $r \equiv r^{-1}(\mod p)$ and $r^2 \equiv 1(\mod p)$ implies that $r \equiv \pm 1(\mod p)$ which are not primitive roots if $p > 3$. So for $p > 3$, the primitive roots group in pairs of mutually inverse primitive roots and their total product is congruent to $1(\mod p)$. If $p = 2$ there is only one primitive root, 1. So the least positive residue of the product of all primitive roots is again $1(\mod p)$. If $p = 3$ the only primitive root is $-1 \equiv 2$. In this case, the least positive residue of the product of all primitive roots equal 2.

16. $\mathbb{F}_p^x = mn - 3$ are elements in the field of p elements $-\mathbb{Z}/(p-1)\mathbb{Z} = \mathbb{Z}/2q\mathbb{Z}$. The mapping $x \to 2x$ is a homomorphism which implies that $\mathbb{Z}/2q\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z}$ is also a homomorphism. The kernel is $q^{\mathbb{Z}}/2q\mathbb{Z} = \mathbb{Z}/2\mathbb{Z}$ which has order 2. So, the image is a subgroup of index 2, and so has order q, and so s generated by any non-zero element. In multiplicative language, squares in $\mathbb{F}_p^x$ form a subgroup of order

q generated by any element whose square is not 1. Each $a, 1 < a < p-1$ is such an element. For such $a, \mathrm{ord}_p a^2 = q$. As $\mathrm{ord}_p(p-1) = 2, p-1$ is not a square. So, $(p-1)a^2 \notin (\#_p^x)^2$ for some $1 < a < p-1$. But its square is a^4 which also generates a^2. So $< (p-1)a^2 >$ must be all of $\#_p^x$, so $(p-1)a^2 = p - a^2$ is primitive.