Solutions

Department of Mathematics

University of Pittsburgh

MATH 1020 (Number theory)

Midterm 2, Fall 2018

Instructor: Kiumars Kaveh

Last Name: **Student Number:**

First Name:

TIME ALLOWED: 1 HOUR AND 30 MINUTES. TOTAL POINTS: 100
NO AIDS ALLOWED. WRITE SOLUTIONS ON THE SPACE PROVIDED.
PLEASE READ THROUGH THE ENTIRE TEST BEFORE STARTING
AND TAKE NOTE OF HOW MANY POINTS EACH QUESTION IS WORTH.
FOR FULL MARK YOU MUST PRESENT YOUR SOLUTION CLEARLY.

Question	Mark
1	/20
2	/10
3	/15
4	/15
5	/10
6	/20
7	/10
8	2
TOTAL	/100 + 2 bonus

1(a).[10 points] Define the following: (1) Euler ϕ function and, (2) a Mersenne prime.

(1) $\phi(n) = |\{x \mid 1 \leq x \leq n, \ x \in \mathbb{N} \ \text{and} \ (x,n)=1\}|$

(2) A prime number q that is of the form $q = 2^p - 1$ is a Mersenne prime.
(If $q = 2^p - 1$ is prime, then p should be prime too)

1(b).[10 points] State the following theorems: (1) Fermat's little theorem, (2) Möbius inversion formula.

(1) $\forall p$ prime & $\forall a \in \mathbb{Z}$ we have
$a^p \equiv a \pmod{p}$.

(2) $\forall$ arithmetic function $f(n)$ with summatory function $F(n)$ we have:

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right)$$

where μ is the Möbius function defined by:

$$\mu(n) = \begin{cases} 1 & n=1 \\ (-1)^r & n = p_1 \cdots p_r, \ p_i \text{ distinct} \\ 0 & \text{otherwise} \end{cases}$$

2.[10 points] Prove that for a prime p and $n > 0$ we have $\phi(p^n) = (p-1)p^{n-1}$.

$\phi(p^n) = p^n - |\{x \mid 1 \le x \le p^n, \; p \mid x\}|$

But number of $1 \le x \le p^n$ which are div. by p is equal to $\frac{p^n}{p} = p^{n-1}$.

Thus: $\phi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$.

3(a).[5 points] Let F be the summatory function of the Möbius function μ, i.e.

$$F(n) = \sum_{d|n} \mu(d).$$

Compute $F(2200)$. (Note $2200 = 8 \cdot 25 \cdot 11$.)

Let 1 denote the constant function 1

i.e. $1(n) = 1 \quad \forall n \in \mathbb{N}$.

Then $F = 1 * \mu$.

But by Möbius inversion we know that 1 & μ are inverse of each other with resp. to Dirichlet product $*$. Thus

$1 * \mu = \varepsilon$ where $\varepsilon(n) = \begin{cases} 1 & n=1 \\ 0 & n \neq 1 \end{cases}$.

Thus $F(2200) = 0$.

(b).[10 points] Let $\tau(n)$ (respectively $\sigma(n)$) denote the number of positive divisors (respectively sum of positive divisors) of n. Compute the following: $\tau(2 \cdot 5 \cdot 17)$ and $\sigma(3 \cdot 2^3)$. (Don't need to simplify your answer.)

$\tau(2 \cdot 5 \cdot 17) = \tau(2)\ \tau(5)\ \tau(17) =$

$2 \cdot 2 \cdot 2 = 8$

$\sigma(3 \cdot 2^3) = \sigma(3)\,\sigma(2^3) = \left(\frac{3^2-1}{3-1}\right)\left(\frac{2^4-1}{2-1}\right)$

$= 4 \cdot 15 = 60$.

4.[15 points] Show that $n = 561 = 3 \cdot 11 \cdot 17$ is a pseudoprime to the base $b = 2$, i.e. $b^n \equiv b \ (mod\ n)$.

$$2^{561} \equiv (2^2)^{280} \cdot 2 \equiv 1^{280} \cdot 2 \equiv 2 \pmod 3$$

$$2^{561} \equiv (2^{10})^{56} \cdot 2 \equiv 1^{56} \cdot 2 \equiv 2 \pmod{11}$$

$$2^{561} \equiv (2^{16})^{35} \cdot 2 \equiv 1^{35} \cdot 2 \equiv 2 \pmod{17}$$

Since 3, 11, 17 are all mutually relatively prime

then $2^{561} \equiv 2 \pmod{3 \cdot 11 \cdot 17 = 561}$.

5.[10 points] Decipher the message EOOF, which was encrypted using the affine transformation $C = 3P + 24$ $(mod\ 26)$ with text blocks of size 1 (i.e. individual letters). (Recall that P and C stand for plaintext and cipher text respectively.)

To convert a text to a number we let $A = 0$, $B = 1$, $C = 2$, $D = 3$, $E = 4$, $F = 5$, $G = 6$, $H = 7$, $I = 8$, $J = 9$, $K = 10$, $L = 11$, $M = 12$, $N = 13$, $O = 14$, $P = 15$, $Q = 16$, $R = 17$, $S = 18$, $T = 19$, $U = 20$, $V = 21$, $W = 22$, $X = 23$, $Y = 24$, $Z = 25$.

$3x \equiv 1 \pmod{26} \Rightarrow x \equiv 9 \pmod{26}$

EOOF $\rightsquigarrow$ 4 14 14 5

First subtract 24 (or add 2) mod 26:

6 16 16 7

Then multiply by 9 (mod 26):

2 14 14 11

↓ ↓ ↓ ↓

C O O L

6(a).[10 points] In the RSA encryption algorithm, $n = 77$ and the encryption key $e = 11$ is used. Find the decryption key d.

$n = 77 = 7 \cdot 11$

$\phi(n) = \phi(7)\,\phi(11) = 6 \cdot 10 = 60$

$e = 11 \rightsquigarrow d = 11^{-1} \bmod 60.$

$\phi(60) = 16$

$d \equiv 11^{15} \equiv (11^2)^7 \cdot 11 \equiv 1^7 \cdot 11 \equiv 11 \pmod{60}$

So $d = 11$.

(b).[10 points] Verify that 2 is a primitive root mod $p = 11$, that is, order of 2 modulo 11 is 10. Using $r = 2$ and $p = 11$, explain how Alice and Bob can use Diffie-Hellman Key Exchange (also called Key Agreement) to agree on an integer x, $1 \leq x < 11$.

$2^2 \equiv 4 \pmod{11} \Rightarrow 2^5 \equiv (-1) \bmod 11$

$\Rightarrow 2^2$ & $2^5 \not\equiv 1 \pmod{11}$ & 2,5 only non-trivial divisors of $\phi(11) = 10$.

so $\operatorname{ord}_{11}(2) = 10$ & hence 2 prim. root mod 11.

Alice chooses Y_1 s.t. $0 < Y_1 < p$ & sends $r^{Y_1} \bmod p$ to Bob.

Bob also chooses Y_2 s.t. $0 < Y_2 < p$ & sends $r^{Y_2} \pmod p$ while calculates $r^{Y_1 Y_2} \pmod p$.

Alice can find Y_2 through knowing Y_1 & r^{Y_2}.

7.[10 points] Use Möbius inversion to prove that for any $n \geq 1$ we have:

$$\sum_{d|n} \mu(d) \cdot \frac{n}{d} = \phi(n).$$

(Hint: recall that in class we proved a theorem/formula for the summatory function of ϕ.)

We know: $\sum_{d|n} \phi(n) = n$ $\rightsquigarrow$ Let us call the identity function by I i.e. $I(n)=n$.

Applying Möbius inversion we get:

$$\mu * I = \phi$$

That is, $\sum_{d|n} \mu(d) \cdot \frac{n}{d} = \phi(n)$ $\forall n \in \mathbb{N}$.

8.[2 points] Draw yourself taking this exam!