ANNA ADARSH COLLEGE FOR WOMEN

24PMSMT1E1 – NUMBER THEORY AND CRYPTOGRAPHY

ANSWER KEY

SECTION - A

1.

$$\begin{array}{r} \text{KD } \frac{\text{MLP}}{\text{SAD}} \\ \text{SAD}\,\overline{|\text{HAPPY}} \\ \underline{\text{GYBE}} \\ \text{COLY} \\ \underline{\text{CCAJ}} \\ \text{MLP} \end{array}$$

2. The Euclidean algorithm works as follows. To find $g.c.d.(a, b)$, where $a > b$, we first divide b into a and write down the quotient q_1 and the remainder r_1: $a = q_1 b + r_1$. Next, we perform a second division with b playing the role of a and r_1 playing the role of b: $b = q_2 r_1 + r_2$. Next, we divide r_2 into r_1: $r_1 = q_3 r_2 + r_3$. We continue in this way, each time dividing the last remainder into the second-to-last remainder, obtaining a new quotient and remainder. When we finally obtain a remainder that divides the previous remainder, we are done: that final nonzero remainder is the greatest common divisor of a and b.

3. **Definition.** Let n be a positive integer. The *Euler phi-function* $\varphi(n)$ is defined to be the number of nonnegative integers b less than n which are prime to n:

$$\varphi(n) \underset{\text{def}}{=} \left| \{0 \le b < n \mid g.c.d.(b, n) = 1\} \right|.$$

4. $x = 6 + 7n$, n is any integer.

5. $2^4 \cdot 3^2 \cdot 7 \cdot 13 \cdot 31 \cdot 601$

6. **Definition.** A *generator* g of a finite field $\mathbf{F}_q$ is an element of order $q-1$; equivalently, the powers of g run through all of the elements of $\mathbf{F}_q^*$.

7. **The Legendre symbol.** Let a be an integer and $p > 2$ a prime. We define the *Legendre symbol* $\left(\frac{a}{p}\right)$ to equal 0, 1 or -1, as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } p|a; \\ 1, & \text{if } a \text{ is a quadratic residue } mod\ p; \\ -1, & \text{if } a \text{ is a nonresidue } mod\ p. \end{cases}$$

---

8. **The Jacobi symbol.** Let a be an integer, and let n be any positive odd number. Let $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ be the prime factorization of n. Then we define the *Jacobi symbol* $\left(\frac{a}{n}\right)$ as the product of the Legendre symbols for the prime factors of n:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_r}\right)^{\alpha_r}.$$

---

9. An enciphering transformation is a function that takes any plaintext message unit and gives us a ciphertext message unit. In other words, it is a map f from the set P of all possible plaintext message units to the set C of all possible ciphertext message units.

---

10. We suppose that our plaintext and ciphertext message units are two-letter blocks called digraphs. This means that the plaintext is split up into two-letter segments.

---

11. To assure message origin and integrity i.e., that the message comes from the claimed sender and has not been altered; to detect forgeries.

---

12. A hash function is an easily computable map f : x → h from a very long input x to a much shorter output h that has the following property: it is not computationally feasible to find two different inputs x and x' such that f(x) = f(x').

SECTION B

13. **Solution.** Since $\binom{n}{m} = \binom{n}{n-m}$, without loss of generality we may assume that $m \leq n/2$. Let us use the following procedure to compute $\binom{n}{m} = n(n-1)(n-2)\cdots(n-m+1)/(2\cdot 3\cdots m)$. We have $m-1$ multiplications followed by $m-1$ divisions. In each case the maximum possible size of the first number in the multiplication or division is $n(n-1)(n-2)\cdots(n-m+1) < n^m$, and a bound for the second number is n. Thus, by the same argument used in the solution to Example 6, we see that a bound for the total number of bit operations is $2(m-1)m([log_2 n]+1)^2$, which for large m and n is essentially $2m^2(log_2 n)^2$.

14.

Solution:

$$\begin{aligned} 1547 &= 2 \cdot 560 + 427 \\ 560 &= 1 \cdot 427 + 133 \\ 427 &= 3 \cdot 133 + 28 \\ 133 &= 4 \cdot 28 + 21 \\ 28 &= 1 \cdot 21 + 7. \end{aligned}$$

Since $7|21$, we are done: $g.c.d.(1547, 560) = 7$.

$$\begin{aligned} 7 &= 28 - 1 \cdot 21 = 28 - 1(133 - 4 \cdot 28) \\ &= 5 \cdot 28 - 1 \cdot 133 = 5(427 - 3 \cdot 133) - 1 \cdot 133 \\ &= 5 \cdot 427 - 16 \cdot 133 = 5 \cdot 427 - 16(560 - 1 \cdot 427) \\ &= 21 \cdot 427 - 16 \cdot 560 = 21(1547 - 2 \cdot 560) - 16 \cdot 560 \\ &= 21 \cdot 1547 - 58 \cdot 560. \end{aligned}$$

15.

Proposition I.3.5. *If* $g.c.d.(a, m) = 1$, *then* $a^{\varphi(m)} \equiv 1 \ mod \ m$.

Proof. We first prove the proposition in the case when m is a prime power: $m = p^\alpha$. We use induction on α. The case $\alpha = 1$ is precisely Fermat's Little Theorem (Proposition I.3.2). Suppose that $\alpha \geq 2$, and the formula holds for the $(\alpha - 1)$-st power of p. Then $a^{p^{\alpha-1}-p^{\alpha-2}} = 1 + p^{\alpha-1}b$ for some integer b, by the induction assumption. Raising both sides of this equation to the p-th power and using the fact that the binomial coefficients in $(1+x)^p$ are each divisible by p (except in the 1 and x^p at the ends), we see that $a^{p^\alpha - p^{\alpha-1}}$ is equal to 1 plus a sum with each term divisible by p^α. That is, $a^{\varphi(p^\alpha)} - 1$ is divisible by p^α, as desired. This proves the proposition for prime powers.

Finally, by the multiplicativity of φ, it is clear that $a^{\varphi(m)} \equiv 1 \ mod \ p^\alpha$ (simply raise both sides of $a^{\varphi(p^\alpha)} \equiv 1 \ mod \ p^\alpha$ to the appropriate power). Since this is true for each $p^\alpha || m$, and since the different prime powers have no common factors with one another, it follows by Property 5 of congruences that $a^{\varphi(m)} \equiv 1 \ mod \ m$.

16.

Proposition II.1.1. *The order of any $a \in \mathbf{F}_q^*$ divides $q-1$.*

First proof. Let d be the smallest power of a which equals 1. (Note that there is a finite power of a that is 1, since the powers of a in the finite set $\mathbf{F}_q^*$ cannot all be distinct, and as soon as $a^i = a^j$ for $j > i$ we have $a^{j-i} = 1$.) Let $S = \{1, a, a^2, \ldots, a^{d-1}\}$ denote the set of all powers of a, and for any $b \in \mathbf{F}_q^*$ let bS denote the "coset" consisting of all elements of the form ba^j (for example, $1S = S$). It is easy to see that any two cosets are either identical or distinct (namely: if some b_1a^i in b_1S is also in b_2S, i.e., if it is of the form b_2a^j, then *any* element $b_1a^{i'}$ in b_1S is of the form to be in b_2S, because $b_1a^{i'} = b_1a^ia^{i'-i} = b_2a^{j+i'-i}$). And each coset contains exactly d elements. Since the union of all the cosets exhausts $\mathbf{F}_q^*$, this means that $\mathbf{F}_q^*$ is a disjoint union of d-element sets; hence $d|(q-1)$.

Second proof. First we show that $a^{q-1} = 1$. To see this, write the product of all nonzero elements in $\mathbf{F}_q$. There are $q-1$ of them. If we multiply each of them by a, we get a rearrangement of the same elements (since any two distinct elements remain distinct after multiplication by a). Thus, the product is not affected. But we have multiplied this product by a^{q-1}. Hence $a^{q-1} = 1$. (Compare with the proof of Proposition I.3.2.) Now let d be the order of a, i.e., the smallest positive power which gives 1. If d did not divide $q-1$, we could find a smaller positive number r — namely, the remainder when $q-1 = bd+r$ is divided by d — such that $a^r = a^{q-1-bd} = 1$. But this contradicts the minimality of d. This concludes the proof.

17.

Solution. The matrix form of the system (a) is $AX \equiv B \ mod\ 26$, where A is the matrix in Example 1, $X = \binom{x}{y}$, and $B = \binom{1}{2}$. We obtain the unique solution

$$X \equiv A^{-1}B \equiv \begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \end{pmatrix} \equiv \begin{pmatrix} 10 \\ 11 \end{pmatrix} \ mod\ 26.$$

18.

Solution. The numerical equivalent of "NOANSWER" is the sequence of vectors $\binom{13}{14}\binom{0}{13}\binom{18}{22}\binom{4}{17}$. We have

$$C = AP = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}\begin{pmatrix} 13 & 0 & 18 & 4 \\ 14 & 13 & 22 & 17 \end{pmatrix} = \begin{pmatrix} 68 & 39 & 102 & 59 \\ 203 & 104 & 302 & 164 \end{pmatrix}$$
$$= \begin{pmatrix} 16 & 13 & 24 & 7 \\ 21 & 0 & 16 & 8 \end{pmatrix},$$

i.e., the coded message is "QVNAYQHI."

---

19. Most of the number theory based cryptosystems for message transmission are deterministic, in the sense that a given plaintext will always be encrypted into the same ciphertext any time it is sent. However, deterministic encryption has two disadvantages:

(1) if an Eavesdropper knows that the plaintext message belongs to a small set (for example, the message is either "yes" or "no"), then she can simply encrypt all possibilities in order to determine which is the supposedly secret message; and

(2) it seems to be very difficult to prove anything about the security of a system if the encryption is deterministic.

For these reasons, probabilistic encryption was introduced.

SECTION C

20.

Solution. To compute $\sum_{i+j=\nu} a_i b_j$, which is the coefficient of x^ν in the product polynomial (here $0 \le \nu \le n_1 + n_2$) requires at most $n_2 + 1$ multiplications and n_2 additions. The numbers being multiplied are bounded by m, and the numbers being added are each at most m^2; but since we have to add the partial sum of up to n_2 such numbers we should take $n_2 m^2$ as our bound on the size of the numbers being added. Thus, in computing the coefficient of x^ν the number of bit operations required is at most

$$(n_2 + 1)(log_2 m + 1)^2 + n_2(log_2(n_2 m^2) + 1).$$

Since there are $n_1 + n_2 + 1$ values of ν, our time estimate for the polynomial multiplication is

$$(n_1 + n_2 + 1)\big((n_2 + 1)(log_2 m + 1)^2 + n_2(log_2(n_2 m^2) + 1)\big).$$

A slightly less rigorous bound is obtained by dropping the 1's, thereby obtaining an expression having a more compact appearance:

$$\frac{n_2(n_1 + n_2)}{log\,2}\left(\frac{(log\,m)^2}{log\,2} + (log\,n_2 + 2\log\,m)\right).$$

21.

Solution. Let n be a k-bit integer written in binary. The conversion algorithm is as follows. Divide $10 = (1010)_2$ into n. The remainder — which will be one of the integers 0, 1, 10, 11, 100, 101, 110, 111, 1000, or 1001 — will be the ones digit d_0. Now replace n by the quotient and repeat the process, dividing that quotient by $(1010)_2$, using the remainder as d_1 and the quotient as the next number into which to divide $(1010)_2$. This process must be repeated a number of times equal to the number of decimal digits in n, which is $\left[\frac{\log n}{\log 10}\right]+1 = O(k)$. Then we're done. (We might want to take our list of decimal digits, i.e., of remainders from all the divisions, and convert them to the more familiar notation by replacing 0, 1, 10, 11, ..., 1001 by 0, 1, 2, 3, ..., 9, respectively.) How many bit operations does this all take? Well, we have $O(k)$ divisions, each requiring $O(4k)$ operations (dividing a number with at most k bits by the 4-bit number $(1010)_2$). But $O(4k)$ is the same as $O(k)$ (constant factors don't matter in the big-O notation), so we conclude that the total number of bit operations is $O(k) \cdot O(k) = O(k^2)$. If we want to express this in terms of n rather than k, then since $k = O(\log n)$, we can write

$$\text{Time(convert } n \text{ to decimal)} = O(\log^2 n).$$

22.

Proposition I.3.2 (Fermat's Little Theorem). *Let p be a prime. Any integer a satisfies $a^p \equiv a \bmod p$, and any integer a not divisible by p satisfies $a^{p-1} \equiv 1 \bmod p$.*

Proof. First suppose that $p \nmid a$. We first claim that the integers $0a, 1a, 2a, 3a, \ldots, (p-1)a$ are a complete set of residues modulo p. To see this, we observe that otherwise two of them, say ia and ja, would have to be in the same residue class, i.e., $ia \equiv ja \bmod p$. But this would mean that $p|(i-j)a$, and since a is not divisible by p, we would have $p|i-j$. Since i and j are both less than p, the only way this can happen is if $i = j$. We conclude that the integers $a, 2a, \ldots, (p-1)a$ are simply a rearrangement of $1, 2, \ldots, p-1$ when considered modulo p. Thus, it follows that the product of the numbers in the first sequence is congruent modulo p to the product of the numbers in the second sequence, i.e., $a^{p-1}(p-1)! \equiv (p-1)! \bmod p$. Thus, $p|\big((p-1)!(a^{p-1}-1)\big)$. Since $(p-1)!$ is not divisible by p, we have $p|(a^{p-1}-1)$, as required. Finally, if we multiply both sides of the congruence $a^{p-1} \equiv 1 \bmod p$ by a, we get the first congruence in the statement of the proposition in the case when a is not divisible by p. But if a is divisible by p, then this congruence $a^p \equiv a \bmod p$ is trivial, since both sides are $\equiv 0 \bmod p$. This concludes the proof of the proposition.

Proposition II.2.4.

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \bmod 8; \\ -1 & \text{if } p \equiv \pm 3 \bmod 8. \end{cases}$$

Proof. Let $f(n) = (-1)^{(n^2-1)/8}$ for n odd, $f(n) = 0$ for n even. We want to show that $(\frac{2}{p}) = f(p)$. Of the various ways of proving this, we shall use an efficient method based on what we already know about finite fields. Since $p^2 \equiv 1 \bmod 8$ for any odd prime p, we know that the field $\mathbf{F}_{p^2}$ contains a primitive 8-th root of unity. Let $\xi \in \mathbf{F}_{p^2}$ denote a primitive 8-th root of 1. Note that $\xi^4 = -1$. Define $G = \sum_{j=0}^{7} f(j)\xi^j$. ($G$ is an example of what is called a *Gauss sum.*) Then $G = \xi - \xi^3 - \xi^5 + \xi^7 = 2(\xi - \xi^3)$ (because $\xi^5 = \xi^4\xi = -\xi$ and $\xi^7 = -\xi^3$), and $G^2 = 4(\xi^2 - 2\xi^4 + \xi^6) = 8$. Thus, in $\mathbf{F}_{p^2}$ we have

$$G^p = (G^2)^{(p-1)/2}G = 8^{(p-1)/2}G = \left(\frac{8}{p}\right)G = \left(\frac{2}{p}\right)G,$$

by Proposition II.2.2 and Proposition II.2.3(c). On the other hand, using the definition of G, the fact that $(a+b)^p = a^p + b^p$ in $\mathbf{F}_{p^2}$, and the obvious observation that $f(j)^p = f(j)$, we compute: $G^p = \sum_{j=0}^{7} f(j)\xi^{pj}$. Notice that $f(j) = f(p)f(pj)$, as we easily check. Then, making the change of variables $j' = pj$ (i.e., modulo 8 we have j' running through $0, \ldots, 7$ when j does), we obtain:

$$G^p = \sum_{j=0}^{7} f(p)f(pj)\xi^{pj} = f(p)\sum_{j'=0}^{7} f(j')\xi^{j'} = f(p)G.$$

Comparing the two equalities for G^p gives the desired result. (Notice that we can divide by G, since it is not 0 in $\mathbf{F}_{p^2}$, as is clear from the fact that its square is 8.)

24.

Solution. We know that plaintexts are enciphered by means of the rule $C \equiv aP + b \ mod\ 729$, and that ciphertexts can be deciphered by means of the rule $P \equiv a'C + b' \ mod\ 729$; here a, b form the enciphering key, and a', b' form the deciphering key. We first want to find a' and b'. We know how three digraphs are deciphered, and, after we replace the digraphs by their numerical equivalents, this gives us the three congruences:

$$675a' + b' \equiv 134 \ mod\ 729,$$
$$216a' + b' \equiv 512 \ mod\ 729,$$
$$238a' + b' \equiv 721 \ mod\ 729.$$

If we try to eliminate b' by subtracting the first two congruences, we arrive at $459a' \equiv 351 \ mod\ 729$, which does not have a unique solution $a' \ mod\ 729$ (there are 27 solutions). We do better if we subtract the third congruence from the first, obtaining $437a' \equiv 142 \ mod\ 729$. To solve this, we must find the inverse of 437 modulo 729. By way of review of the Euclidean algorithm, let's go through that in detail:

$$729 = 437 + 292$$
$$437 = 292 + 145$$
$$292 = 2 \cdot 145 + 2$$
$$145 = 72 \cdot 2 + 1$$

and then

$$\begin{aligned} 1 &= 145 - 72 \cdot 2 \\ &= 145 - 72(292 - 2 \cdot 145) \\ &= 145 \cdot 145 - 72 \cdot 292 \\ &= 145(437 - 292) - 72 \cdot 292 \\ &= 145 \cdot 437 - 217 \cdot 292 \\ &= 145 \cdot 437 - 217(729 - 437) \\ &\equiv 362 \cdot 437 \ mod\ 729. \end{aligned}$$

Thus, $a' \equiv 362 \cdot 142 \equiv 374 \ mod\ 729$, and then $b' \equiv 134 - 675 \cdot 374 \equiv 647 \ mod\ 729$. Now applying the deciphering transformation to the digraphs "ND", "XB" and "HO" of our message — they correspond to the integers 354, 622 and 203, respectively — we obtain the integers 365, 724 and 24. Writing $365 = 13 \cdot 27 + 14$, $724 = 26 \cdot 27 + 22$, $24 = 0 \cdot 27 + 24$, we put together the plaintext digraphs into the message "NO WAY". Finally, to find the enciphering key we compute $a \equiv a'^{-1} \equiv 374^{-1} \equiv 614 \ mod\ 729$ (again using the Euclidean algorithm) and $b \equiv -a'^{-1}b' \equiv -614 \cdot 647 \equiv 47 \ mod\ 729$.

25.

RSA Cryptosystem

The RSA cryptosystem is a widely used public-key encryption technique based on the difficulty of factoring large prime numbers. It was developed in 1977 by Rivest, Shamir, and Adleman.

Key Generation Steps:

1. Choose two large prime numbers p and q.
2. Compute $n=p\times q$, which is used as the modulus.
3. Calculate $\phi(n)=(p-1)(q-1)$.
4. Select a public key e, where $1<e<\phi(n)$ and $\gcd(e,\phi(n))=1$.
5. Compute the private key d, the modular inverse of e such that $e\times d\equiv 1 \pmod{\phi(n)}$.

Encryption:
For a plaintext message M, the ciphertext is

$$C = M^e mod\ n$$

Decryption:
To recover the message:

$$M = C^d mod\ n$$

Features:

- Security relies on the mathematical difficulty of factoring large numbers.
- Provides both encryption and digital signatures.
- Used in secure communication, banking, and internet protocols (e.g., SSL/TLS).

Limitation:
It is computationally slower compared to symmetric algorithms, hence often combined with them (e.g., in hybrid cryptosystems).