1. [10]	2. [10]	3. [10]	4. [10]	5. [10]
6. [10]	7. [10]	8. [10]	9. [10]	10. [10]
Total. [100]				

MA 503 **Midterm** **March 22, 2021**

Name: ***Solutions***

Open book and notes. *Answers must include supporting work.*

Calculators and wolfram alpha can be used for basic computations.

(1) [10 pts] Prove that the congruence $6x^2+5x+1 \equiv_p 0$ has a solution for every prime p, even though $6x^2+5x+1=0$ has no integer solutions. [Hint. $p=2,3$ are special because 6 is not a unit modulo 2 or 3.]

Solution: Clearly,

$$6x^2+5x+1=(3x+1)(2x+1)=0$$

has no integer solutions. If $p=2$, then the congruence

$$6x^2+5x+1 \equiv_2 x+1 \equiv 0$$

has a solution 1. If $p=3$, then the congruence

$$6x^2+5x+1 \equiv_2 2x+1 \equiv 0$$

has a solution 1. If $p>3$, then using quadratic formula we get two solutions

$$x=\tfrac{1}{12}(-5\pm\sqrt{1})=\tfrac{-5\pm 1}{12}.$$

The expression above makes sense modulo $p>3$ because 12 is coprime to p. Actually, the obtained expression gives us $-\frac{1}{2}$ and $-\frac{1}{3}$ which is not a big surprise because $6x^2+5x+1=(3x+1)(2x+1)$.

(2) [10 pts] Solve the following system of congruences:

$$\begin{cases} x \equiv_2 1 \\ x \equiv_3 2 \\ x \equiv_5 0 \\ x \equiv_7 3 \end{cases}$$

Solution: We can solve subsystems one by one. For instance, we can find a solution for a subsystem

$$\begin{cases} x \equiv_5 0 \\ x \equiv_7 3 \end{cases}$$

by enumerating solutions for the second congruence and choose one satisfying the first congruence: $3, 10, \ldots$. $x \equiv_{35} 10$ works. Then consider

$$\begin{cases} x \equiv_3 2 \\ x \equiv_{35} 10 \end{cases}$$

and a sequence $10, 45, 80$ $x \equiv_{105} 80$ works for both congruences. Finally, consider a system

$$\begin{cases} x \equiv_2 1 \\ x \equiv_{105} 80 \end{cases}$$

and get $x \equiv_{210} 185$ which is the answer.

(3) [10 pts] Consider the group U_{15}. What elements does it contain? For each non-trivial element a find $|a|$ and the subgroup $\langle a \rangle$ it generates. Using the obtained data, prove that U_{15} is not cyclic.

Solution: $U_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}$.

$$\begin{aligned} \langle 1 \rangle &= \{1\} & |1| &= 1 \\ \langle 2 \rangle &= \{1, 2, 4, 8\} & |2| &= 4 \\ \langle 4 \rangle &= \{1, 4\} & |4| &= 2 \\ \langle 7 \rangle &= \{1, 7, 4, 13\} & |7| &= 4 \\ \langle 8 \rangle &= \{1, 8, 4, 2\} & |8| &= 4 \\ \langle 11 \rangle &= \{1, 11\} & |11| &= 2 \\ \langle 13 \rangle &= \{1, 13, 4, 7\} & |13| &= 4 \\ \langle 14 \rangle &= \{1, 14\} & |14| &= 2. \end{aligned}$$

Since $\langle a \rangle \neq U_{15}$ for any $a \in U_{15}$, the group U_{15} is not cyclic.

(4) [10 pts] Suppose that $g^a \equiv_n 1$ and $g^b \equiv_n 1$. Prove that $g^{\gcd(a,b)} \equiv_n 1$.

Solution: It easily follows from the Bezout identity because

$$\gcd(a,b) = \alpha a + \beta b \text{ for some } \alpha, \beta \in \mathbb{Z}$$

Therefore, $g^{\gcd(a,b)} \equiv_n g^{\alpha a + \beta b} = g^{\alpha a} g^{\beta b} = (g^a)^\alpha \left(g^b\right)^\beta = 1 \cdot 1 = 1.$

(5) [10 pts] Use the Pohlig–Hellman algorithm to find the discrete logarithm $\log_7(166)$ modulo 433. (To compute $x_i = \log_{g_i}(h_i)$ simply enumerate sufficiently many powers of g_i.)

Solution: 7 is a primitive root of a prime 433 and $|a| = 432 = 2^4 \cdot 3^3$.

$N_1 = 27$ $\quad g_1 = 7^{27} \equiv_{433} 265$ $\quad h_1 = 166^{27} \equiv_{433} 250$ $\quad \log_{265}(250) = x_1$

$N_2 = 16$ $\quad g_2 = 7^{16} \equiv_{433} 374$ $\quad h_2 = 166^{16} \equiv_{433} 335$ $\quad \log_{335}(335) = x_2$.

Compute powers of 265 until we get 250:

$265^0 \equiv_N 1$ $\quad 265^1 \equiv_N 265$ $\quad 265^2 \equiv_N 79$ $\quad 265^3 \equiv_N 151$ $\quad 265^4 \equiv_N 179$

$265^5 \equiv_N 238$ $\quad 265^6 \equiv_N 285$ $\quad 265^7 \equiv_N 183$ $\quad 265^8 \equiv_N 432$ $\quad 265^9 \equiv_N 168$

$265^{10} \equiv_N 354$ $\quad 265^{11} \equiv_N 282$ $\quad 265^{12} \equiv_N 254$ $\quad 265^{13} \equiv_N 195$ $\quad 265^{14} \equiv_N 148$

$265^{15} \equiv_N 250$.

Compute powers of 374 until we get 335:

$374^0 \equiv_N 1$ $\quad 374^1 \equiv_N 374$ $\quad 374^2 \equiv_N 17$ $\quad 374^3 \equiv_N 296$ $\quad 374^4 \equiv_N 289$

$374^5 \equiv_N 269$ $\quad 374^6 \equiv_N 150$ $\quad 374^7 \equiv_N 243$ $\quad 374^8 \equiv_N 385$ $\quad 374^9 \equiv_N 234$

$374^{10} \equiv_N 50$ $\quad 374^{11} \equiv_N 81$ $\quad 374^{12} \equiv_N 417$ $\quad 374^{13} \equiv_N 78$ $\quad 374^{14} \equiv_N 161$

$374^{15} \equiv_N 27$ $\quad 374^{16} \equiv_N 139$ $\quad 374^{17} \equiv_N 26$ $\quad 374^{18} \equiv_N 198$ $\quad 374^{19} \equiv_N 9$

$374^{20} \equiv_N 335$

Hence, $x_1 = 15$ and $x_2 = 20$. Solve the system

$$\begin{cases} x \equiv_{16} 15 \\ x \equiv_{27} 20 \end{cases}$$

to get $x \equiv_{432} 47$.

(6) [10 pts] Here is an example of a public key system that was proposed at a cryptography conference. It is supposed to be faster and more efficient than RSA.

(Key generation) Alice chooses two large primes p and q and she publishes $N = pq$. It is assumed that N is hard to factor. Alice also chooses three random numbers g, r_1, and r_2 modulo N and computes

$$g_1 = g^{r_1(p-1)} \ \% \ N \quad \text{and} \quad g_2 = g^{r_2(q-1)} \ \% \ N.$$

Her public key is the triple (N, g_1, g_2) and her private key is the pair of primes (p, q).

(Encryption) Bob wants to send the message m to Alice, where m is a number modulo N. He chooses two random integers s_1 and s_2 modulo N and computes

$$c_1 = mg_1^{s_1} \ \% \ N \quad \text{and} \quad c_2 = mg_2^{s_2} \ \% \ N.$$

Bob sends the ciphertext (c_1, c_2) to Alice.

(Decryption) Alice uses the Chinese remainder theorem to solve the pair of congruences

$$\begin{cases} x \equiv_p c_1, \\ x \equiv_q c_2. \end{cases}$$

(a) Prove that Alice's solution x is equal to Bob's plaintext m.

(b) Explain why this cryptosystem is not secure.

Solution: To show (a) it is sufficient to notice that m is the solution to the system above because

$$mg_1^{s_1} \equiv_N m\left(g^{r_1(p-1)}\right)^{s_1} \equiv_N m\left(g^{(p-1)}\right)^{r_1 s_1} \equiv_p m$$
$$mg_2^{s_2} \equiv_N m\left(g^{r_2(q-1)}\right)^{s_2} \equiv_N m\left(g^{(q-1)}\right)^{r_2 s_2} \equiv_q m$$

Hence, Alice, indeed, gets m.

Similarly, we have

$$g_1 \equiv_p g^{r_1(p-1)} \equiv_p 1$$
$$g_2 \equiv_q g^{r_2(q-1)} \equiv_q 1.$$

Hence, $p = \gcd(g_1 - 1, N)$ and $q = \gcd(g_2 - 1, N)$.

(7) [10 pts] Perform the following encryptions and decryptions using the Goldwasser–Micali public key cryptosystem.

(a) [4 pts] Bob's public key is the pair $N = 1842338473$ and $a = 1532411781$. Alice encrypts three bits and sends Bob the ciphertext blocks

$$1794677960,\ 525734818,\ \text{and } 420526487.$$

Decrypt Alice's message using the factorization $N = pq = 32411 \cdot 56843$.

Solution: Compute the Legendre symbols using the Euler's criterion:

$$(1794677960/32411) = (16068/32411) = 16068^{\frac{32411-1}{2}} \ \% \ 32411 = 32410 \equiv -1.$$

$$(525734818/32411) = (28398/32411) = 28398^{\frac{32411-1}{2}} \ \% \ 32411 = 1.$$

$$(420526487/32411) = (26173/32411) = 26173^{\frac{32411-1}{2}} \ \% \ 32411 = 32410 \equiv -1.$$

Hence, Alice encrypted 101.

(b) [3 pts] Bob's public key is $N = 3149$ and $a = 2013$. Alice encrypts three bits and sends Bob the ciphertext blocks 2322, 719, and 202. Unfortunately, Bob used primes that are much too small. Factor N and decrypt Alice's message.

Solution: Factor $N = 3149 = 47 \cdot 67$ and proceed as in item (a).

$$(2322/47) = (19/47) = 19^{\frac{47-1}{2}} \ \% \ 47 = 46 \equiv -1.$$

$$(719/47) = (14/47) = 14^{\frac{47-1}{2}} \ \% \ 47 = 1.$$

$$(202/47) = (14/27) = 14^{\frac{47-1}{2}} \ \% \ 47 = 1.$$

Hence, Alice encrypted 100.

(c) [3 pts] Bob's public key is $N = 781044643$ and $a = 568980706$. Encrypt the three bits 1, 1, 0 using, respectively, the three random values $r = 705130839$, $r = 631364468$, $r = 67651321$.

Solution:

$$c = 568980706 \cdot 705130839^2 \ \% \ 781044643 = 517254876$$

$$c = 568980706 \cdot 631364468^2 \ \% \ 781044643 = 4308279$$

$$c = 67651321^2 \ \% \ 781044643 = 660699010.$$

(8) [10 pts] Let $n = 1729$.

(a) [5 pts] Show that n is a Carmichael number.

Solution: $n = 1729 = 7 \cdot 13 \cdot 19$ is composite and $\varphi(n) = 6 \cdot 12 \cdot 18 = 1296$. We need to check that every unit a modulo n satisfies the following $a^{1296} \equiv_n 1$ which is equivalent to the system of congruences

$$\begin{cases} a^{1296} \equiv_7 1 \\ a^{1296} \equiv_{13} 1 \\ a^{1296} \equiv_{19} 1 \end{cases}$$

And those congruences hold because $7, 13, 19$ are prime numbers and by Fermat's little theorem $a^6 \equiv_7 1$, $a^{12} \equiv_{13} 1$, $a^{18} \equiv_{19} 1$ and so

$$\begin{cases} a^{1296} = (a^6)^{216} \equiv_7 1, \\ a^{1296} = (a^{12})^{108} \equiv_{13} 1, \\ a^{1296} = (a^{18})^{72} \equiv_{19} 1 \end{cases}$$

(b) [5 pts] Check if $a = 3$ is a Miller–Rabin witness for the compositeness of n.

Solution: $n - 1 = 1728 = 2^6 \cdot 3^3$ and we check the following powers of 3

$$\begin{aligned} 3^{1728} &\equiv_{1729} 1 \\ 3^{864} &\equiv_{1729} 1 \\ 3^{432} &\equiv_{1729} 1 \\ 3^{216} &\equiv_{1729} 1 \\ 3^{108} &\equiv_{1729} 1 \\ 3^{54} &\equiv_{1729} 1 \\ 3^{27} &\equiv_{1729} 664. \end{aligned}$$

Therefore, 3 is a witness for compositness.

(9) [10 pts] For $N = 52907$ use the following data:

$$399^2 \equiv_N 480 = 2^5 \cdot 3 \cdot 5,$$
$$763^2 \equiv_N 192 = 2^6 \cdot 3,$$
$$773^2 \equiv_N 15552 = 2^6 \cdot 3^5,$$
$$976^2 \equiv_N 250 = 2 \cdot 5^3,$$

to find values of a and b satisfying $a^2 \equiv_N b^2$ and then compute $\gcd(N, a - b)$ in order to find a nontrivial factor of N.

Solution: Here we need to take an appropriate product of the given identities to have squares on the left and on the right. For instance, product of the second and third identities give

$$763^2 \cdot 773^2 \equiv_N 2^{12} \cdot 3^6$$
$$7822 \equiv_N (763 \cdot 773)^2 \equiv_N (64 \cdot 27)^2$$

Then $\gcd(6094, 52907) = 277$ which is one of the factors of N. Another one is 191.

(10) [20 pts] Let $n = 113$.

(a) [5 pts] Is 2 a primitive root modulo n?

Solution: $\varphi(n) = 112 = 2^4 \cdot 7$. If 2 is a primitive root, then

$$2^{56} \equiv_{113} 1 \quad \text{or} \quad 2^{16} \equiv_{113} 1.$$

and, indeed,

$$2^{56} \equiv_{113} 1.$$

Hence, it is not a primitive root.

(b) [5 pts] Find $|3|$ in U_n.

Solution: $|3|$ is a divisor of 112, but since

$$3^{56} \equiv_{113} 112 \neq 1, \quad \text{and} \quad 3^{16} \equiv_{113} 49 \neq 1,$$

$|3| = 112$.