

MATH 482: MIDTERM EXAM SOLUTIONS

1. Find the largest Latin square contained in the multiplication table of \mathbb{Z}_{12} . Is your answer orthogonal to the addition table of \mathbb{Z}_4 ?

Answer: The largest Latin square contained in the multiplication table of \mathbb{Z}_n is the multiplication table of \mathbb{Z}_n^\times . Since:

$$\mathbb{Z}_{12}^\times = \{1, 5, 7, 11\}$$

the Latin square is:

1	5	7	11
5	1	11	7
7	11	1	5
11	7	5	1

Comparing this to the addition table of \mathbb{Z}_4 :

0	1	2	3
1	2	3	0
2	3	0	1
3	0	1	2

we see that they are not orthogonal because there are repeats in the set of ordered pairs. For example, in the first row second column we have the ordered pair (5,1), and in the second row, first column we also have (5,1).

2. On a certain island, every inhabitant is either a knight or a knave. Knights always tell the truth and knaves always lie. You meet two such inhabitants A and B .

A says: "It is not true that B and I are both knaves."

B says: " A is lying."

Write down a system of equations over \mathbb{Z}_2 and solve it to determine the identities of A and B .

Answer:

$$A = (A + 1)(B + 1) + 1 = AB + A + B$$

$$B = A + 1$$

So:

$$AB = A + 1$$

The only solution to this equation is $A = 1$, $B = 0$, so A is a knight and B is a knave.

3. Use cyclotomic polynomials to find the prime factorization of $531440 = 3^{12} - 1$.

Answer:

$$x^{12} - 1 = \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_4(x)\Phi_6(x)\Phi_{12}(x) = (x^6 - 1)(x^6 + 1)$$

$$\text{Recall that: } x^6 - 1 = (x^3 - 1)(x^3 + 1) = (x - 1)(x^2 + x + 1)(x + 1)(x^2 - x + 1)$$

$$= \Phi_1(x)\Phi_3(x)\Phi_2(x)\Phi_6(x)$$

$$\text{and: } x^6 + 1 = \Phi_4(x)\Phi_{12}(x)$$

$$\text{But } x^6 + 1 = (x^2)^3 + 1 = (x^2 + 1)(x^4 - x^2 + 1)$$

Therefore:

$$3^{12} - 1 = (2)(4)(13)(10)(7)(73) = 2^4 \cdot 5 \cdot 7 \cdot 13 \cdot 73$$

4. (a) Show that $x^2 + 1$ is irreducible in $\mathbb{Z}_7[x]$.

(b) Assuming that $x^2 + 1 = 0$ in \mathbb{F}_{49} , prove that $(x + 1)^4 = 3$ and $(x + 1)^{24} = 1$ in \mathbb{F}_{49} .

Answer:

(a) The squares in \mathbb{Z}_7 are 0, 1, 4, 2, 2, 4, 1. Since $x^2 = 6$ has no solutions in \mathbb{Z}_7 , $x^2 + 1$ is irreducible in $\mathbb{Z}_7[x]$.

$$(b) (x + 1)^2 = x^2 + 2x + 1 = 2x$$

$$(x + 1)^4 = 4x^2 = -4 = 3$$

$$(x + 1)^{24} = 3^6 = (3^2)^3 = 2^3 = 1$$

5. Alice has a safe which is opened by a secret 3-digit number x . She wants to securely communicate this number to Bob and Carol in such a way that they cannot open the safe unless they work together.

Bob's public key is $(n, e) = (8, 3)$ and Carol's public key is $(n', e') = (125, 67)$.

(a) Alice sends Bob the message $c = 5$. Find the decrypted message a .

(b) Alice sends Carol the message $c' = 7$. Find the decrypted message a' .

(c) If $x \pmod{n} = a$ and $x \pmod{n'} = a'$, use the Chinese remainder theorem to help them find the secret number x .

$$\text{Hint: } 8(47) - 125(3) = 376 - 375 = 1$$

Answer:

(a) Since $\phi(8) = 4$, we have $d = 3^{-1} \pmod{4}$. Since $3 \cdot 3 = 1 \pmod{4}$, $d = 3$. Therefore:

$$a = 5^3 \pmod{8} = 5$$

(b) Since $\phi(125) = 100$, we have $d' = 67^{-1} \pmod{100}$.

$$100 = 67 + 33$$

$$67 = 33(2) + 1$$

$$1 = 67 - 33(2) = 67 - 2(100 - 67) = 67(3) - 2(100).$$

Therefore, $d' = 3$, so:

$$a' = 7^3 \pmod{125} = 93.$$

$$(c) \ x = a + 376(a' - a) = 5 + 376(88) \pmod{1000} = 093$$

Notice that Alice did not succeed. Carol could have opened the safe without Bob!

6. Let $s(d)$ denote the sum of the positive divisors of d .

(a) Prove that:

$$n = \sum_{d|n} s(d)\mu(n/d)$$

(b) Consider a solid cube with a special vertex v and look at the eight sections of this cube that contain v :

0-dimensional section: the vertex v .

1-dimensional sections: the three edges coming out of v .

2-dimensional sections: the three faces meeting at v .

3-dimensional section: the whole cube.

For each vertex u of the cube, find the number of *even* dimensional sections listed above that contain u . Also, find the number of *odd* dimensional sections listed above that contain u . Explain how this gives a second proof of part (a) if $n = pqr$ where p, q , and r are distinct primes.

Hint: Draw the divisor graph for $n = 30$.

Answer:

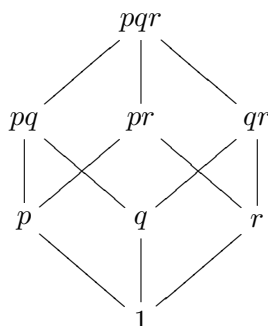
(a) By definition:

$$s(n) = \sum_{d|n} d$$

By the Möbius inversion formula:

$$n = \sum_{d|n} s(d)\mu(n/d)$$

(b) The positive divisors of $n = pqr$ are: $1, p, q, r, pq, pr, qr, pqr$ and the divisor graph is:



Let $v = 1$ be the special vertex.

The even dimensional sections that contain 1 are as follows: the vertex 1 itself, and the three faces corresponding to divisors of pq , pr , and qr .

The odd dimensional sections that contain 1 are as follows: the whole cube, and the three edges corresponding to divisors of p , q , and r .

The vertex 1 is contained in 4 odd dimensional sections and 4 even dimensional sections.

The vertices p , q and r are each contained in 2 even dimensional sections and 2 odd dimensional sections.

The vertices pq , pr , and qr are each contained in 1 even dimensional section and 1 odd dimensional section.

However, the vertex pqr is contained in 1 odd dimensional section, but no even dimensional sections.

Now let's look at the right hand side of the formula:

$$-s(1) + s(p) + s(q) + s(r) - s(pq) - s(pr) - s(qr) + s(pqr)$$

A vertex of the divisor graph appears in this sum whenever it is contained in one of the above sections containing 1 (and its sign is positive if the section is odd dimensional, negative if the section is even dimensional). Since every vertex (except pqr) appears the same number of times in odd and even dimensional sections, they will all cancel out, and just leave pqr .