

MATH 4000/6000 Exam 1 Solutions

1. Use the Binomial Theorem to prove the formula

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots + (-1)^n \binom{n}{n} = 0$$

for all $n \in \mathbb{N}$. *Hint:* $(1 - 1)^n = ?$.

The Binomial Theorem states

$$(x + y)^n = \binom{n}{0} x^n y^0 + \binom{n}{1} x^{n-1} y^1 + \binom{n}{2} x^{n-2} y^2 + \cdots + \binom{n}{n} x^0 y^n.$$

Let $x = 1$ and $y = -1$. Then we have

$$\begin{aligned} (1 + (-1))^n &= \binom{n}{0} 1^n (-1)^0 + \binom{n}{1} 1^{n-1} (-1)^1 + \binom{n}{2} 1^{n-2} (-1)^2 + \cdots + \binom{n}{n} 1^0 (-1)^n, \\ 0 &= \binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots + (-1)^n \binom{n}{n}. \end{aligned}$$

2. Prove the following divisibility test. If $n \in \mathbb{N}$, then 11 divides n if and only if 11 divides the alternating sum of the digits of n . (For example, let $n = 91806$. The alternating sum of the digits of n is $9 - 1 + 8 - 0 + 6 = 22$, and $11|22$, so $11|91806$.)

Suppose n has k digits, and let a_i be the digit of n in the i th place, $i = 0, 1, \dots, k - 1$ ($n = a_{k-1}a_{k-2} \dots a_1a_0$). Thus

$$n = a_0(10)^0 + a_1(10)^1 + \cdots + a_{k-2}(10)^{k-2} + a_{k-1}(10)^{k-1}.$$

Now we look at this equation modulo 11. Since $10 \equiv -1 \pmod{11}$, we obtain

$$\begin{aligned} n &\equiv a_0(-1)^0 + a_1(-1)^1 + \cdots + a_{k-2}(-1)^{k-2} + a_{k-1}(-1)^{k-1} \pmod{11}, \\ n &\equiv a_0 - a_1 + \cdots + (-1)^{k-2}a_{k-2} + (-1)^{k-1}a_{k-1} \pmod{11}. \end{aligned}$$

Thus $11|n$ if and only if $11|(a_0 - a_1 + \cdots + (-1)^{k-2}a_{k-2} + (-1)^{k-1}a_{k-1})$.

3. Use the Chinese Remainder Theorem to solve the following simultaneous congruence: $x \equiv 4 \pmod{12}$, $x \equiv 22 \pmod{39}$.

First note that $\gcd(12, 39) = 3$, and $3|(22 - 4)$, so there is a solution x , and x is defined modulo $\text{lcm}(12, 39) = 156$.

The substitution $y = x - 4$ gives the simultaneous congruence $y \equiv 0 \pmod{12}$, $y \equiv 18 \pmod{39}$.

The substitution $z = y/3$ gives $z \equiv 0 \pmod{4}$, $z \equiv 6 \pmod{13}$, and the solution z is defined modulo $4 \cdot 13 = 52$. Now $\gcd(4, 13) = 1$, and by inspection (without using the Euclidean algorithm) we see that $1 \cdot 13 - 3 \cdot 4 = 1$. Therefore $-3 \cdot 4 \equiv 1 \pmod{13}$, and so $z = -3 \cdot 4 \cdot 6$ satisfies our two congruences.

Thus the solution is $z \equiv -72 \pmod{52}$, or $z \equiv 32 \pmod{52}$.

So $y \equiv 96 \pmod{156}$, and finally $x \equiv 100 \pmod{156}$.

Check: $100 \equiv 4 \pmod{12}$, $12|(100 - 4)$, $12|96$, $12 \cdot 8 = 96$.

$100 \equiv 22 \pmod{39}$, $39|100 - 22$, $39|78$, $39 \cdot 2 = 78$.

4. Let p be a prime number.

(a) Prove that if $a \in \mathbb{N}$, and p does not divide a , then $\gcd(p, a) = 1$.

Since p is prime, its only positive divisors are 1 and p . By hypothesis p is not a divisor of a . Thus the only positive common divisor of p and a is 1. Therefore 1 is the greatest common divisor of p and a .

(b) Use part (a) to show that every nonzero element \bar{a} of \mathbb{Z}_p has a unique inverse.

Suppose $\bar{a} \neq 0$ in \mathbb{Z}_p . This means that p does not divide a , so by part (a) we have that $\gcd(p, a) = 1$. Therefore there are integers s and t such that $sp + ta = 1$. This gives $\bar{t} \cdot \bar{a} = \bar{1}$ in \mathbb{Z}_p . Since $ta = at$ we also have $\bar{a} \cdot \bar{t} = \bar{1}$. So \bar{t} is an inverse of \bar{a} .

Now suppose \bar{a} has two inverses \bar{t} and \bar{u} . Then $\bar{t} = \bar{t} \cdot \bar{1} = \bar{t} \cdot (\bar{a} \cdot \bar{u}) = (\bar{t} \cdot \bar{a}) \cdot \bar{u} = \bar{1} \cdot \bar{u} = \bar{u}$. Thus \bar{a} has a unique inverse.

(c) Which nonzero elements of \mathbb{Z}_p are their own inverses? (Solve the equation $\bar{a}^2 = \bar{1}$.)

$$\begin{aligned}\bar{a}^2 &= \bar{1} \\ \bar{a}^2 - \bar{1} &= \bar{0} \\ (\bar{a} - \bar{1})(\bar{a} + \bar{1}) &= \bar{0} \\ \bar{a} - \bar{1} = \bar{0} \text{ or } \bar{a} + \bar{1} &= \bar{0} \\ \bar{a} = \bar{1} \text{ or } \bar{a} = -\bar{1} &= \overline{p-1}\end{aligned}$$

(d) Using parts (b) and (c), compute the product of all the nonzero elements of \mathbb{Z}_p . (For example, in \mathbb{Z}_5 the product of all the nonzero elements is $\bar{1} \cdot \bar{2} \cdot \bar{3} \cdot \bar{4} = \overline{24} = \bar{4}$.)

The product of all the nonzero elements of \mathbb{Z}_p is $\bar{1} \cdot \bar{2} \cdots \overline{(p-2)} \cdot \overline{(p-1)}$. By part (c), the first factor $\bar{1}$ and the last factor $\overline{p-1}$ are their own inverses, and the product $\bar{2} \cdots \overline{(p-2)}$, contains as factors every other nonzero element of \mathbb{Z}_p as well as its inverse. So the product $\bar{2} \cdots \overline{(p-2)}$ equals $\bar{1}$, and hence we have $\bar{1} \cdot \bar{2} \cdots \overline{(p-2)} \cdot \overline{(p-1)} = \bar{1} \cdot \bar{1} \cdot \overline{(p-1)} = \overline{p-1} = -\bar{1}$.

5. Let $M_2(\mathbb{Z})$ be the ring of 2×2 matrices with integer entries.

(a) Give an example of a zero-divisor in $M_2(\mathbb{Z})$. (Prove that it is a zero-divisor.)

A zero-divisor in $M_2(\mathbb{Z})$ is a non-zero matrix A such that there exists a matrix B with $AB = 0$. Let

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix},$$

and let $B = A$. Then

$$AB = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

(b) Give an example of a unit in $M_2(\mathbb{Z})$. (Prove that it is a unit.)

A unit in $M_2(\mathbb{Z})$ is a matrix A such that there exists a matrix B with $AB = I$ and $BA = I$. Let

$$A = B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

the identity matrix. Then $AB = I \cdot I = I$.

6. Prove or give a counterexample:

(a) If $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_m$ and $\bar{a} \neq \bar{0}$, then $\bar{a} \cdot \bar{b} = \bar{a} \cdot \bar{c}$ implies $\bar{b} = \bar{c}$.

False. Here is a counterexample. Let $m = 6$, $a = 3$, $b = 2$, and $c = 4$. Then $\bar{a} \cdot \bar{b} = \bar{3} \cdot \bar{2} = \bar{6} = \bar{0}$, and $\bar{a} \cdot \bar{c} = \bar{3} \cdot \bar{4} = \bar{12} = \bar{0}$, but $\bar{b} \neq \bar{c}$.

(b) If R is a ring and $a, b, c \in R$ satisfy $ab = 1$ and $ca = 1$, then a must be a unit.

True. To prove that a is a unit, we must show that there is an element $b \in R$ such that $ab = 1$ and $ba = 1$. So it's enough to show that if $ab = 1$ and $ca = 1$, then $b = c$. We make the following computation:

$$\begin{aligned} ab &= 1 \\ c(ab) &= c(1) \\ (ca)b &= c \\ (1)b &= c \\ b &= c \end{aligned}$$

(c) Every nonzero element of a commutative ring is either a unit or a zero-divisor.

False. Here is a counterexample. Consider the commutative ring \mathbb{Z} of integers. The units of \mathbb{Z} are $+1$ and -1 . (If $a, b \in \mathbb{Z}$ and $ab = 1$, then $a = b = 1$ or $a = b = -1$.) But \mathbb{Z} has no zero-divisors. (If $a, b \in \mathbb{Z}$ and $ab = 0$, then $a = 0$ or $b = 0$.) So, for example, $2 \in \mathbb{Z}$ is neither a unit nor a zero-divisor.