MID-TERM EXAM

Answer all of the questions **1** to **10** (4 points each).

1. *Find the value of* $(n, n+1)$ *and* $[n, n+1]$ *for each integer* $n \geq 1$.

For each integer $n \geq 1$, $n + 1 - n = 1$, hence $(n, n+1) = 1$ and $[n, n+1] = n(n+1)$.

2. *Prove that if* $a \mid b$ *then* $|a| \leq |b|$ *or* $b = 0$.

If $a \mid b$ then $b = qa$ for some integer q, so $b = 0$ if $q = 0$, otherwise $|q| \geq 1$ and $|b| = |q| \cdot |a| \geq |a|0$.

3. *Find all the pairs of integers* u, v *such that* $17u - 13v = 1$.

$$17 = 13 + 4, \quad 13 = 4 \cdot 3 + 1, \quad 1 = 13 - 4 \cdot 3 = 13 - (17 - 13) \cdot 3 = 17(-3) + 13(4) = 17(13t - 3) + 13(4 - 17t)$$

Therefore $17u - 13v = 1$ if and only if $(u, v) \in \{(13t - 3, 4 - 17t) : t \in \mathbb{Z}\}$.

4. *Fill in the blank:* "If d divides ab and $(d, a) = 1$, then ...".

Then d divides b. For if $dx + ay = 1$ and $dq = ab$ then $d(bx + qy) = dbx + dqy = dbx + aby = (dx + ay)b = b$.

5. *Give the exact definition of* $r \equiv s \bmod n$.

$r \equiv s \bmod n$ if and only if n divides $r - s$, that is if and only if $r = qn + s$ for some integer q.

6. *Precisely state the fundamental theorem of arithmetic.*

If $n \neq 0, \pm 1$ is an integer then $n = \pm p_1^{\nu_1} \cdots p_r^{\nu_r}$, where the p_i are distinct primes and the $\nu_i \geq 1$. Moreover, this factorization is unique in the following sense. If $n = \pm q_1^{\eta_1} \cdots q_s^{\eta_s}$, where the q_i are distinct primes and the $\eta_i \geq 1$, then $r = s$ and, after suitable relabelling, $p_i = q_i$, $\nu_i = \eta_i$, $i = 1, \ldots, r = s$.

7. *Find all the integers* x *such that* $4x \equiv -1 \bmod 5$ *and* $3x \equiv 5 \bmod 7$.

By the Chinese remainder theorem, there is a solution for x modulo 35. Notice that $x \equiv 1 \bmod 5$, $x \equiv 5 \bmod 7$, and 11 satisfies both congruences. Therefore $x = 11 + 35t, t \in \mathbb{Z}$ are all of the solutions.

8. *Fill in the blank:* "If $da \equiv db \bmod m$ then $a \equiv b \bmod$ ...".

Then $a \equiv b \bmod m/(d, m)$. For if $(d, m) = g$, $d = gd', m = gm'$, we have $gm' \mid gd'(a - b)$, hence $m' \mid d'(a - b)$. Now $(d', m') = 1$ so $m' \mid a - b$ (see question 4).

9. *Precisely state Fermat's little theorem.*

If a is an integer, p is a prime and $(a, p) = 1$, then $a^{p-1} \equiv 1 \bmod p$.

10. *What is the smallest residue of* $2^{558} \bmod 31$*?*

Note that $558 = 2 \cdot 3^2 \cdot 31$. Now $2^{2 \cdot 3^2} \equiv 4^{3 \cdot 3} \equiv 64^3 \equiv 2^3 \bmod 31$. Now 31 is prime and $(2, 31) = 1$, so $2^{31} \equiv 2 \bmod 31$ by Fermat's little theorem. Hence $2^{2 \cdot 3^2 \cdot 31} \equiv 2^{3 \cdot 31} \equiv 2^3 \equiv 8 \bmod 31$.

Answer both questions **11** and **12** (15 points each).

11. *Prove the fundamental theorem of arithmetic.*

The integer 2 may be written as a product of primes. Let n be an integer greater than 2, and suppose that the integers $2, \ldots, n-1$ may be written as products of primes. Now n is either prime or $n = ab$, where $1 < a, b < n$, and by assumption a and b may be written as products of primes. Hence n may be written as a product of primes. By induction, any integer $n > 1$ may be written as a product of primes.

Now suppose $p_1 \cdots p_r = q_1 \cdots q_s$, where the p_i, q_i are primes, not necessarily distinct, but $p_i \neq q_j$ for at least one pair i, j. Then we may assume that $p_i \neq q_j$ for every pair i, j, for we may divide both sides by any $p_i = q_j$ if such i, j exist. Now $p_1 \mid q_1 \cdots q_s$, so $p_1 \mid q_i$ for some i, say $i = 1$. These are primes, so $p_1 = q_1$, a contradiction.

12. *Prove Fermat's little theorem.*

Let p be a prime and a an integer with $(a, p) = 1$. We claim that $\{1, 2 \ldots, p-1 \bmod p\} = \{a, 2a, \ldots, (p-1)a \bmod p\}$. For if $ka \equiv 0 \bmod p$ then $k \equiv kaa^{-1} \equiv 0 \bmod p$, and if $ka \equiv k'a \bmod p$ then $k \equiv kaa^{-1} \equiv k'aa^{-1} \equiv k' \bmod p$, hence there are $p-1$ distinct nonzero elements in the second set. By our claim, we have $1 \cdot 2 \cdots (p-1) \equiv a \cdot 2a \cdots (p-1)a \equiv a^{p-1} 1 \cdot 2 \cdots (p-1) \bmod p$. Each of $1, 2, \ldots, p-1$ is coprime to p and hence invertible modulo p. Multiplying both sides of the above congruence by $2^{-1} \cdots (p-1)^{-1}$, we obtain $1 \equiv a^{p-1} \bmod p$.

Answer three of the questions **13** to **22** (10 points each).

13. *Show that if $a > b \geq 1$ then there exist integers q, r such that $a = qb + r$, where $0 \leq r \leq b-1$ and q and r are unique.*

Certainly there exists a unique integer q such that $qb \leq a < (q+1)b$. (Consider $\{n \in \mathbb{N} : a - nb \geq 0\}$, which is not empty as it contains 1, and let q be the largest element in this set.) Let $r = a - qb$. Then $0 \leq r < (q+1)b - qb = b$, that is $0 \leq r \leq b-1$, and $a = qb + r$. Suppose $a = qb + r = q'b + r'$, with $0 \leq r, r' \leq b-1$. Then $r - r' = b(q - q')$. Now if $r - r' > 0$ then $q - q' > 0$, and $a = qb + r > q'b + r' = a$, which is absurd. Similarly if $r - r' < 0$. Hence $r - r' = 0$ and $q - q' = 0$, that is q, r are unique.

14. *Prove that the set of integers $\{9a + 23b : a, b \in \mathbb{Z}\}$ is the same as the set of integers $\{5c + 9d : c, d \in \mathbb{Z}\}$ (without computing gcds).*

First fix integers a, b. We seek integers c, d such that $9a + 23b = 5c + 9d$, that is $5c = 9a + 23b - 9d$. Let $d = a - 3b$. Then $9a + 23b - 9d = 50b$, and $c = 10b$ is an integer. Now fix integers c, d, and let $a = d - 2c, b = c$. Then $9a + 23b = 9d - 18c + 23c = 9d + 5c$. We have given a bijection between the two sets.

15. *Prove that there are infinitely many primes of the from $4m + 3$, where m is an integer.*

Suppose $p_1, \ldots, p_n$ are all of the primes of the form $4m + 3$, and let $N = 4p_1 \cdots p_n - 1$. Then N has only odd prime factors, that is primes of the form $4m + 1$ or $4m + 3$. Now $(4k + 1)(4m + 1) = 4(4km) + 4(k + m) + 1$, so a product of odd primes not equal to $4m + 3$ is of the form $4m + 1$. Hence N must have at least one prime factor of the form $4m + 3$. We are assuming $p_1, \ldots, p_n$ are all of them, so $p_i \mid N$ for some i. Then $p_i \mid 4p_1 \cdots p_n - N = 1$, which is absurd.

16. *Prove that if $f(x)$ is a polynomial with integer coefficients, and a, b are integers such that $a \equiv b \bmod m$, then $f(a) \equiv f(b) \bmod m$.*

Suppose $f(x) = c_n x^n + \cdots + c_0$. Then $f(a) - f(b) = c_n(a^n - b^n) + \cdots + c_1(a - b)$. Now $c_n(a^n - b^n) \equiv c_n(a - b)(a^{n-1} + a^{n-1}b + \cdots + b^{n-1}) \equiv 0 \bmod m$, and similarly all the terms of $f(a) - f(b)$ are congruent to 0 mod m, hence $f(a) - f(b) \equiv 0 \bmod m$, that is $f(a) \equiv f(b) \bmod m$.

17. *Prove Wilson's theorem.*

Let p be prime. Each $r \not\equiv 0 \bmod p$ has a unique inverse $r^{-1} \bmod p$, and $r^{-1} \equiv r \bmod p$ if and only if $1 \equiv r^2 \bmod p$ if and only if $p \mid (r^2 - 1) = (r + 1)(r - 1)$ if and only if $p \mid r + 1$ or $p \mid r - 1$ if and only if $r \equiv \pm 1 \bmod p$. Therefore

$1 \cdot 2 \cdots (p-1) \equiv 1 \cdot 2 \cdot 2^{-1} \cdots (p-2)(p-2)^{-1}(p-1) \equiv p-1 \equiv -1 \bmod p$.

Now suppose a is not prime. Then $(a-1)! \equiv 0 \bmod p$ for any prime p dividing a. On the other hand, if $(a-1)! \equiv -1 \bmod a$ then $(a-1)! \equiv -1 \bmod p$, which is absurd.

Therefore $(p-1)! \equiv -1 \bmod p$ if and only if p is prime.

18. *Prove the Chinese remainder theorem.*

Let $a_1, \ldots, a_n$ be pairwise coprime integers. Then $(a_1 \cdots a_n/a_i, a_i) = 1$ for each i, so there exist integers v_i, w_i such that $v_i a_1 \cdots a_n/a_i - w_i a_i = 1$. Note that $v_i a_1 \cdots a_n/a_i \equiv 1 \bmod a_i$, $v_i a_1 \cdots a_n/a_i \equiv 0 \bmod a_j$ for each $j \neq i$. Then $x = \sum_{i=1}^{n} b_i v_i a_1 \cdots a_n/a_i \equiv b_i \bmod a_i$ for each i. Now suppose $y \equiv x \equiv b_i \bmod a_i$ for each i. that is $y - x \equiv 0 \bmod a_i$ for each i. Then $y - x \equiv 0 \bmod [a_1, \ldots, a_n] = a_1 \cdots a_n$. Conversely if $y \equiv x \bmod a_1 \cdots a_n$, then $y \equiv x \equiv b_i \bmod a_i$ for each i. We have proved that the system of congruences $x \equiv b_i \bmod a_i$ for pairwise coprime integers $a_1, \ldots, a_n$ has a unique solution modulo $a_1 \ldots a_n$.

19. *Prove that if* $(a, m) = 1$ *then there exists an integer* b *such that* $ab \equiv 1 \bmod m$.

If $(a, m) = 1$ then there exist integers b, n such that $ab - mn = 1$, that is $ab = 1 + mn \equiv 1 \bmod m$.

20. *Prove that if* $x^2 \equiv 1 \bmod pq$ *has exactly 4 solutions* $\bmod pq$ *for odd primes* $p \neq q$.

We want $x^2 - 1 \equiv (x+1)(x-1) \equiv 0 \bmod pq$. Then $p \mid x+1$ or $x-1$ and $q \mid x+1$ or $x-1$, but neither p nor q divides both $x+1$ and $x-1$, for otherwise p or q divides $x+1-(x-1) = 2$, which is absurd as p, q are odd. Therefore there are at most $2 \cdot 2 = 4$ solutions to our equation, according as $x \equiv \pm 1 \bmod p$, $x \equiv \pm 1 \bmod q$. Let a, b be integers such that $ap - bq = 2$ (which exist since $(p, q) = 1$), and let $x = ap - 1 = bq + 1$. Then $(\pm x)^2 = x^2 = (ap-1)(bq+1) = abpq + ap - bq - 1 = abpq + 2 - 1 \equiv 1 \bmod pq$. $x = 1, pq - 1$ are obviously two more solutions. All four solutions we have found are distinct, for $x \equiv -x \bmod pq$ implies $2x \equiv 0 \bmod pq$, hence $2 \mid pq$, but p, q are odd; if $ap - 1 = bq + 1 = 1$ then $b = 0$, $ap = 2$, which is impossible as $p > 2$; finally if $ap - 1 = bq + 1 = pq - 1$, then $q(p - b) = 2$, which is impossible as $q > 2$.

21. *If* a *and* b *are positive integers such that* $(a, b) = 1$ *and* ab *is a perfect square, prove that* a *and* b *are perfect squares.*

We have $ab = \prod_p p^{2v_p}$, and since $(a, b) = 1$, if $p \mid a$ then $p \nmid b$ and vice-versa. By uniqueness of factorization, we must then have $a = \prod_{p|a} p^{2v_p}$ and $b = \prod_{p|b} p^{2v_p}$ are squares.

22. *Write an essay on something within the scope of the course, including at least one proof not covered by this exam.*