UNIVERSITY OF VICTORIA EXAMINATIONS, DECEMBER 2019

MATHEMATICS 362 SECTION [A01] CRN 12189

ELEMENTARY NUMBER THEORY

Instructor: Dr. C.M. Mynhardt

Name:_____ Student Number:_____

To be answered on the paper. **Duration: 3 hours**

Count the number of pages in this examination paper before beginning to write, and report any discrepancy immediately to the invigilator.

This question paper has **10 pages** plus this cover page and the yellow signature back page.

There are **16** questions, some with several parts.

The Sharp EL-510-R or RNB or RTB is the only calculator permitted.

No other aids such as books, notes, or formula sheets are allowed. Scratch paper will be provided by the invigilator.

Students may not be in possession of receiving/transmitting electronic gadgets of any kind.

Students may not leave the room during the exam without first handing their papers to the invigilator.

Total:

_____

80

1. [1] State the Well Ordering Principle for integers.

   Every non-empty set S of positive integers contains a smallest element. That is, there is some integer $a \in S$ such that $a \leq b$ for each $b \in S$.

2. [4] Prove that every integer n with $n \geq 2$ is divisible by a prime.

   Let S be the set of non-trivial positive divisors of n. If $S = \varnothing$, then n is prime by definition and $n|n$, so the lemma follows.

   If $S \neq \varnothing$, then (by the Well-Ordering Principle) it has a smallest element, say d. If d has a non-trivial positive divisor c, then $c < d$ and $c|n$ (since $c|d$ and $d|n$), which is impossible by the choice of d as the smallest non-trivial positive divisor of n. Thus d is prime and a divisor of n.

3. [1] State the Unique Factorization Theorem (a.k.a. the Fundamental Theorem of Arithmetic) without proving it.

   Every integer $n \geq 2$ can be written as a product of primes in one and only one way.

4. [12] Let p and q be prime numbers, and m and n any positive integers. Determine whether each of the following statements is true or false. If it is true, prove it. If it is false, give a counterexample.

   (a) If $|m-n|=2$ and $m+n$ is a multiple of 12, then m and n are both odd.

   True. Since $|m-n|=2$, $m \equiv n \pmod 2$. Suppose m, n are both even. Since $|m-n|=2$, one of them is congruent to 0 (mod 4) and the other one is congruent to 2 (mod 4). But then $m+n \equiv 2 \pmod 4$ and $m+n \equiv 12 \equiv 0 \pmod 4$, which is impossible.

   (b) If $|m-n|=2$ and $m+n$ is a multiple of 12, then m and n are twin primes.

   False, since $23+25=48$ is a multiple of 12 and $|23-25|=2$, but 25 is not prime.

   (c) If p and q are twin primes such that $p>q>3$, then $p+q$ is a multiple of 12.

   True. Since p and q are primes and $p, q > 3$, we know that p and q are congruent to $\pm 1 \pmod 6$, i.e., $q \equiv -1 \pmod 6$ and $p \equiv 1 \pmod 6$. Say $q=6k-1$ and $p=6k+1$. Then $p+q=12k$, as required.

   (d) If p and q are twin primes, then $pq+1$ is a square.

   True. Assume without loss of generality that $q=p-2$. Then $pq+1=p^2-2p+1=(p-1)^2$.

   (e) If $pq+1$ is a square, then p and q are twin primes.

   True. Suppose $p>q$ and $pq+1=a^2$. Then $a>2$ and $pq=a^2-1=(a-1)(a+1)$, where $a-1, a+1>1$. By the unique factorization theorem, $p=a+1$ and $q=a-1$. Hence $p-q=2$. Since p and q are primes, they are twin primes.

5. [2] Solve the congruence $7x \equiv 42 \pmod{21}$.

Since $(7, 21) = 7$ and $7|42$, there are 7 solutions, namely $0, 3, 6, 9, 12, 15, 18$.

6. [5] Find b, a multiple of 7 that leaves a remainder of 1 when it is divided by each of the numbers $2, 3, 4, 5, 6$, such that $1000 < b < 1500$.

We have

$$\begin{aligned} b &\equiv 1 \pmod{2} \\ b &\equiv 1 \pmod{3} \\ b &\equiv 1 \pmod{4} \\ b &\equiv 1 \pmod{5} \\ b &\equiv 1 \pmod{6} \\ b &\equiv 0 \pmod{7}. \end{aligned}$$

To use the Chinese Remainder Theorem, we must change this system to an equivalent system where the moduli are relatively prime. Note that

$$b \equiv 1 \pmod{4} \Rightarrow b \text{ is odd } \Rightarrow b \equiv 1 \pmod{2}.$$

So the condition that $b \equiv 1 \pmod{2}$ is superfluous. Also, by the Chinese Remainder Theorem,

$$\begin{aligned} &b \equiv 1 \pmod{3} \text{ and } b \equiv 1 \pmod{4} \Leftrightarrow b \equiv 1 \pmod{12} \\ &\Leftrightarrow b = 12s + 1 \text{ for some integer } s \\ &\Leftrightarrow b = 6(2s) + 1 \text{ for some integer } s \\ &\Rightarrow b \equiv 1 \pmod{6}. \end{aligned}$$

So the condition that $b \equiv 1 \pmod{6}$ is also superfluous. Hence the system of congruences

$$\begin{aligned} b &\equiv 1 \pmod{3} && (1) \\ b &\equiv 1 \pmod{4} && (2) \\ b &\equiv 1 \pmod{5} && (3) \\ b &\equiv 0 \pmod{7}, && (4) \end{aligned}$$

in which the moduli are pairwise relatively prime, *is equivalent to* the original system of congruences. So we only need to solve this second system. As above, from (1) and (2), $b = 12s + 1$ for some integer s. Substitute into (3):

$$12s + 1 \equiv 1 \pmod{5} \Rightarrow 2s \equiv 0 \pmod{5} \Rightarrow s \equiv 0 \pmod{5}.$$

Therefore $s = 5t$ for some integer t, which gives $b = 12s + 1 = 12(5t) + 1 = 60t + 1$. Substitute into (4):

$$60t + 1 \equiv 0 \pmod{7} \Rightarrow 4t \equiv -1 \equiv 20 \pmod{7} \Rightarrow t \equiv 5 \pmod{7}.$$

Hence $t = 7q + 5$ for some integer q, which gives $b = 60t + 1 = 60(7q + 5) + 1 = 420q + 301$. When $q = 2$, we have that $b = 1141$, as required.

7. [8] Prove that if n is an even perfect number, then $n = 2^{p-1}(2^p - 1)$, where p and $2^p - 1$ are both prime.

Since n is even, we can write

$$n = 2^e m, \quad \text{where } m \text{ is odd and } e \geq 1. \tag{5}$$

We know that $\sigma(2^e) = 2^{e+1} - 1 \neq 2 \cdot 2^e$, so $n \neq 2^e$; that is, $m > 1$. Since $\sigma(m) \geq 1 + m > m$, we can write

$$\sigma(m) = m + s, \quad \text{where } s > 0. \tag{6}$$

Since n is perfect, $2n = \sigma(n)$, so from (5),

$$2n = 2^{e+1}m = \sigma(n). \tag{7}$$

This is one expression for $\sigma(n)$. From (5) and the multiplicativity of σ,

$$\sigma(n) = \sigma(2^e m) = \sigma(2^e)\sigma(m). \tag{8}$$

But $\sigma(2^e) = 2^{e+1} - 1$, thus also using (6), (8) becomes

$$\sigma(n) = (2^{e+1} - 1)(m + s) = 2^{e+1}m - m + (2^{e+1} - 1)s. \tag{9}$$

This is another expression for $\sigma(n)$.

Combining (7) and (9) gives

$$\begin{aligned} 2^{e+1}m &= 2^{e+1}m - m + (2^{e+1} - 1)s, \\ \text{i.e.} \qquad m &= (2^{e+1} - 1)s. \end{aligned} \tag{10}$$

This means that $s|m$, and since $e \geq 1$, $2^{e+1} - 1 > 1$ and thus $s < m$.

Now look at (6): The sum of all divisors of m is equal to $m + s$. Thus the sum of all divisors of m, excluding m, that is, the sum of all divisors of m less than m, is equal to s. Hence s is a divisor of m and s is less than m, so s is a term of the sum in (6).

But if s is a term in a sum which sums to s, then s is the **only** term in that sum.

Hence s is the only divisor of m that is less than m, and this is only possible if $s = 1$ because $1|m$ always.

Therefore m is prime, and substituting $s = 1$ in (10) we get $m = 2^{e+1} - 1$. The only numbers of this form that can be prime are those in which $e + 1$ is prime. Hence $e + 1 = p$, where p is prime, so $n = 2^{p-1}(2^p - 1)$ for some prime p.

8. [5] Prove that if g is a primitive root of m, then the least residues, modulo m, of $g,\ g^2, ...,\ g^{\phi(m)}$ are a permutation of the elements of $\Phi(m)$.

Since $(g, m) = 1$, $(g^k, m) = 1$ for each $k = 1, 2, ..., \phi(m)$. Thus the least residues of the numbers $g,\ g^2, ...,\ g^{\phi(m)}$ are all relatively prime to m, hence they are elements of $\Phi(m)$. There are $\phi(m)$ numbers $g,\ g^2, ...,\ g^{\phi(m)}$, so we only have to show that no two of them have the same least residues $(\text{mod } m)$.

Suppose

$$g^k \equiv g^j \pmod{m}$$

for some integers $1 \leq k \leq \phi(m)$ and $1 \leq j \leq \phi(m)$. We want to prove that $k = j$.

Since g is a primitive root of m, $\text{ord}_m\, g = \phi(m)$. By Theorem 10.5, $k \equiv j \pmod{\phi(m)}$.

If $k, j < \phi(m)$, then they are least residues $(\text{mod } \phi(m))$ and so they are equal. If one of them, say k, is equal to $\phi(m)$, then the only number in $\{1, 2, ..., \phi(m)\}$ congruent to k is $\phi(m)$, and so $j = \phi(m)$ also.

9. (a) [1] Complete the following form of Euler's criterion for quadratic residues:

If p is an odd prime and $p \nmid a$, then $(a/p) \equiv$ $a^{(p-1)/2} \pmod{p}$.

(b) [2] Prove that if p is prime and $p \equiv 7 \pmod{8}$, then $p|(2^{(p-1)/2} - 1)$.

Since $p \equiv 7 \pmod{8}$, $(2/p) = 1$. Hence $2^{(p-1)/2} \equiv 1 \pmod{p}$, which implies that $p|(2^{(p-1)/2} - 1)$.

(c) [2] Prove that $2^{83} - 1$ is composite without performing the binary operation of divisibility.

Note that 167 is prime: clearly, none of $2, 3, 5, 7, 11$ divides 167, and $13^2 = 169 > 167$. Since $167 \equiv 7 \pmod{p}$, part (b) implies that $167|(2^{83} - 1)$. Hence $2^{83} - 1$ is composite.

10. [5] Prove that 2 is a primitive root of a prime of the form $p = 3 \cdot 2^n + 1$ if and only if $p = 13$.

Suppose $p = 13$. Then $p = 4 \cdot 3 + 1$, and p and 3 are both prime. By a theorem, 2 is a primitive root of 13.

Consider all positive integer values of n except $n = 2$.

If $n = 1$, then $p = 7$. Now, $(2/7) = 1$, and by Euler's Criterion, $1 = (2/7) \equiv 2^3 \pmod{7}$. Hence $\text{ord}_7 2 = 3 < 6$ and 2 is not a primitive root of 7.

Now assume $n \geq 3$. Then $n - 3$ is a nonnegative integer and so

$$p \equiv 3 \cdot 2^n + 1 \equiv 8 \cdot 3 \cdot 2^{n-3} + 1 \equiv 1 \pmod{8}.$$

Hence $(2/p) = 1$ and so $2^{(p-1)/2} \equiv 1 \pmod{p}$ by Euler's Criterion. Hence $\text{ord}_p 2 < p - 1$ and 2 is not a primitive root of p.

11. [8] Let $x = a$, $y = b$, $z = c$ be a fundamental solution of the equation $x^2 + y^2 = z^2$, where a is even. Prove that there are positive integers m and n with $m > n$, $(m, n) = 1$ and $m \not\equiv n \pmod 2$, such that $a = 2mn$, $b = m^2 - n^2$ and $c = m^2 + n^2$.

Since a is even, $a = 2r$ for some r. Thus $a^2 = 4r^2$. But $a^2 + b^2 = c^2$, hence $a^2 = c^2 - b^2$ and so

$$4r^2 = (c + b)(c - b). \tag{11}$$

By a lemma, b and c are odd, so $c + b$ and $c - b$ are both even. Thus there are integers s and t such that

$$c + b = 2s \quad \text{and} \quad c - b = 2t, \tag{12}$$

that is,

$$c = s + t \quad \text{and} \quad b = s - t. \tag{13}$$

Substituting (12) into (11) and dividing by 4, we get

$$r^2 = st.$$

We prove that s and t are squares. By a lemma, we only need to prove that $(s, t) = 1$. Suppose $d|s$ and $d|t$. Then by (13), $d|c$ and $d|b$. But $(b, c) = 1$ and so $d = 1$, that is, $(s, t) = 1$.

Thus let $s = m^2$ and $t = n^2$, where m and n are positive, so as explained above we now have $a = 2mn$. From (13),

$$c = s + t = m^2 + n^2,$$
$$b = s - t = m^2 - n^2.$$

To prove the lemma we must still prove that $m > n$, $(m, n) = 1$ and $m \not\equiv n \pmod 2$. But a, b, c is a fundamental solution, so $b > 0$, hence $m^2 > n^2$, and since m and n are positive, $m > n$.

Suppose $d|m$ and $d|n$. Then $d|s$ and $d|t$, so $d = 1$ since $(s, t) = 1$. Hence $(m, n) = 1$.

Since $(m, n) = 1$, m and n are not both even. Suppose m and n are both odd. Then s and t are both odd, and so by (13), b and c are both even, which is a contradiction.

12. [5] Solve the quadratic congruence $4y^2 + y + 3 \equiv 0 \pmod{17}$ or explain why it doesn't have solutions.

Suppose $4x \equiv 1 \pmod{17}$. Then $4x \equiv -16 \pmod{17}$, hence $x \equiv -4 \pmod{17}$.

Therefore

$$\begin{aligned} 4y^2 + y + 3 \equiv 0 \pmod{17} &\Leftrightarrow y^2 - 4y - 12 \equiv 0 \pmod{17} \\ &\Leftrightarrow y^2 - 4y + 4 \equiv -1 \pmod{17} \\ &\Leftrightarrow (y-2)^2 \equiv -1 \pmod{17}. \end{aligned}$$

Since $17 \equiv 1 \pmod{4}$, $(-1/17) = 1$. Hence the congruence has solutions. Since $-1 \equiv 16 \pmod{17}$, $y - 2 \equiv 4$ or $-4 \pmod{17}$, so $y = 6$ or 15.

13. (a) [3] Find all fundamental Pythagorean triangles with a side of length 40.

Since we are looking for a fundamental triangle, we know that only one side has even length, namely $a = 2mn$, where one of m and n is even and the other one odd. Hence $a = 2(4)(5)$, $b = m^2 - n^2 = 5^2 - 4^2 = 9$ and $c = m^2 + n^2 = 5^2 + 4^2 = 41$. Hence $(40, 9, 41)$ is such a triangle. Also, we have $a = 2(20)(1)$, $b = m^2 - n^2 = 20^2 - 1^2 = 399$ and $c = m^2 + n^2 = 20^2 + 1^2 = 401$. Hence $(40, 399, 401)$ is also such a triangle.
(Test: $40^2 + 9^2 = 41^2$; $40^2 + 399^2 401^2$.)

(b) [3] Find a Pythagorean triangle with hypotenuse of length 120, or explain why such a triangle doesn't exist.

Since $5 = 2^2 + 1^2$, we have the fundamental Pythagorean triangle (a, b, c) with $a = 2 \cdot 2 = 4$, $b = 2^2 - 1^2 = 3$ and $c = 5$. Multiplying a, b, c by 24 gives a triangle (a', b', c') with $a' = 96$, $b' = 72$ and $c' = 120$.
(Test: $96^2 + 72^2 = 14\,400 = 120^2$.)

14. Let $\mathcal{S}$ be the statement "*if* $p \equiv 1 \pmod 4$ *is prime, then* p *is representable as the sum of two squares.*"
Let n be an integer whose prime factorization contains each prime p, where $p \equiv 3 \pmod 4$, to an even power. You want to show that n is representable as the sum of two squares.

(a) [5] Explain (no proofs required) why it is sufficient to prove the statement $\mathcal{S}$.

We know that if x and y are the sums of squares, then xy is the sum of squares. We also know that if x is the sum of squares, then so is k^2x, for any integer k. In addition, any integer n can be written as

$$n = p_1^{2e_1+1}p_2^{2e_2+1}...p_r^{2e_r+1}p_{r+1}^{2e_{r+1}}, ..., p_s^{2e_s}.$$

Since each prime p, where $p \equiv 3 \pmod 4$, occurs to an even power in the prime power decomposition of n, we can write n as

$$n = k^2p_1p_2...p_r \text{ or } n = 2k^2p_1p_2...p_r,$$

where the p_i are distinct primes congruent to $1 \pmod 4$. Hence if we can write each p_i as the sum of two squares, then we can write n so as well.

(b) [5] Now prove $\mathcal{S}$. The proof uses a lemma known as Thue's Lemma. State this lemma without proving it.

Thue's Lemma: Let p be a prime and a an integer such that $(a, p) = 1$. Then the congruence $ax \equiv y \pmod p$ is satisfied by $x = x_0$, $y = y_0$, where $0 < |x_0| < \sqrt{p}$ and $0 < |y_0| < \sqrt{p}$.
Since $p \equiv 1 \pmod 4$, -1 is a quadratic residue $\pmod p$. Thus there exists an integer a satisfying $a^2 \equiv -1 \pmod p$. Then $(a, p) = 1$ (for any common divisor of a and p must also divide -1) and by Thue's Lemma, the congruence $ax \equiv y \pmod p$ is satisfied by x_0, y_0 such that $0 < |x_0|, |y_0| < \sqrt{p}$, i.e., such that

$$0 < x_0^2 + y_0^2 < 2p. \tag{14}$$

But then

$$\begin{array}{lrcll} & (ax_0)^2 & \equiv & y_0^2 \pmod p & \text{because } ax_0 \equiv y_0 \pmod p \\ \text{i.e.} & a^2x_0^2 & \equiv & y_0^2 \pmod p & \\ \text{i.e.} & -x_0^2 & \equiv & y_0^2 \pmod p & \text{because } a^2 \equiv -1 \pmod p. \\ \text{i.e.} & x_0^2 + y_0^2 & \equiv & 0 \pmod p & \end{array}$$

Thus there exists an integer k such that

$$x_0^2 + y_0^2 = kp. \tag{15}$$

By (14), (15) is only possible if $k = 1$, which proves the theorem.

15. (a) [1] Interpret the **Prime Number Theorem** to complete the following statement:

If $x \in \mathbb{R}$ is large enough, then there are approximately $x/\ln x$ *primes less than or equal to x.*

(b) [1] Give an example of a sequence of 10 consecutive integers, all of which are composite.

Consider the ten numbers $11! + 2,\ 11! + 3, ..., 11! + 11$.

(c) [2] Explain why any arithmetic progression of primes has finite length.

For any prime p and any integer $a \geq 2$, the last number in the progression $p,\ p + a,\ p + 2a,\ ...,\ p + pa$ is not prime because it is divisible by p.

16. [5] Suppose p is prime, $(n, p-1) = 1$, and $a \in \Phi(p)$. Use the fact that p has a primitive root to prove that the congruence $x^n \equiv a \pmod{p}$ has exactly one solution. (Finding a solution in terms of a primitive root might be a good idea.)

Let g be a primitive root of p. Since $a \in \Phi(p)$, $a \equiv g^j \pmod{p}$ for some $j \geq 1$.

Since $(n, p-1)$ is prime, the congruence $ny \equiv j \pmod{p-1}$ has a unique solution, say $y = k$. Since $\operatorname{ord}_p g = p - 1$, we know that $g^r \equiv g^s \pmod{p}$ if and only if $r \equiv s \pmod{p-1}$. Hence

$$(g^k)^n \equiv g^{nk} \equiv g^j \equiv a \pmod{p},$$

hence the least residue of g^k is a solution to the given congruence. The solution is unique because k is the unique solution to the congruence $ny \equiv j \pmod{p-1}$.

★ - END - ★