University College of Cape Breton MATH325

Number Theory

Jan-Apr 2005 Time : 13 hours

Attempt all questions at some point during the course

A1. Deduce from the proven result that if a is negative then there still exists a unique quotient and remainder of b on division by a, but now with the proviso that $0 \leq r < |a|$.

A2. Prove that if $d|b_1$, $d|b_2, \ldots d|b_n$ then $d|(\sum_{i=1}^{n} k_i b_i), \forall k_i \in \mathbb{Z}$

A3. Show that $n^{\frac{1}{k}}$ $(n, k \in \mathbb{N})$ is irrational unless $n = a^k$ for some $a \in \mathbb{Z}$.

A4. Evaluate $\gcd(n, kn)$ if $k \in \mathbb{Z}$. What about $\gcd(kn, ln)$?

A5. If $n = (\prod_{i=1}^{k} a_i) + 1$ show that $\gcd(n, a_i) = 1$.

A6. For which $b \in \mathbb{Q}$ is it true that $ab|bc$ implies that $a|c$?

A7. Prove that if $a|c$ and $k|l$ then $ka|lc$.

A8. Is is true that $d|abc$ implies that $d|a$ or $d|b$ or $d|c$? What if we further insist that $d < \min(a, b, c)$? Or if we have just a and b and not c in the question?

A9. Evaluate $\gcd(12, 15)$, $\gcd(26, 45)$ and $\gcd(-54, 42)$. Find x and y in each case such that $\gcd(a, b) = ax + by$.

A10. Use the Euclidean algorithm to find $\gcd(26, 65)$, $\gcd(987, 236)$ and $\gcd(672, 444)$. Find x and y such that $ax + by = \gcd(a, b)$

A11. Either prove impossible or find integer values of x and y such that

$$11x + 18y = 3 \qquad 26x + 8y = 2 \qquad 9x + 12y = 4$$

A12. Find the prime representations of 5 684 and 2 737 and hence find their greatest common divisor.

A13. If $p|n$ and $q|n$ are both distinct primes and $p, q \geq \sqrt[4]{n}$ then $\frac{n}{pq}$ is prime. True or false?

A14. Prove that if n is the product of k consecutive integers then $k!|n$.

A15. Prove that n is composite implies that $2^n - 1$ is composite.

A16. Is it true that if $2^n - 1$ is composite then n is ?

A17. Suppose p is prime and $p|(a^2 - b^2)$ and $p|(c^2 - b^2)$. Either prove or disprove these statements: $p|(a^2 - c^2)$, $p|(a^2 + c^2)$, $p|(a - c)$, $a = kp \pm c$ for some $k \in \mathbb{Z}$.

A18. Prove that the set of numbers of the form $4k + 1$, $k \in \mathbb{Z}$, the Hilbert numbers, is closed under multiplication. Show that unique factorisation does not hold for them.

A19. Disprove these statements:

(a) $2^n + 3$ is prime for all natural numbers n.

(b) $2^{2n} + 7$ is prime for all natural numbers n.

(c) Either $6n + 1$ or $6n - 1$ is prime for any $n \in \mathbb{N}$.

A20. To what least positive residue are 24, -3, 13 congruent modulo 14 ?

A21. Solve these congruences:

$$5x \equiv 15 \bmod 17 \qquad 3x \equiv 2 \bmod 11 \qquad 14x \equiv 12 \bmod 23$$

A22. Solve these three congruences: $2x \equiv 5 \bmod 11$, $2x \equiv 5 \bmod 12$ and $2x \equiv 10 \bmod 10$.

A23. Solve this set of simultaneous congruences:

$$\begin{aligned} x &\equiv 6 \bmod 11 \\ 2x - 4 &\equiv 0 \bmod 3 \\ x + 4 &\equiv 6 \bmod 7 \end{aligned}$$

A24. Show that $(b^m - 1)|(b^{mn} - 1)\ \forall b \in \mathbb{Z}, m, n \in \mathbb{N}$

A25. Given that the most common letters in this sentence are "a" and "r", decode it (we are using an affine encryption and the standard alphabet plus space).

`␣nnfktnfvwxnfaxnumcnfonllqxnbngosh`

A26. If "th" encrypts to `hy` and "e " to `lb` in a 27-letter digraph transform, what does the following sentence read ? `hylbceynibvtedubthkbtebu␣␣vhfmsbhylbioncqzeq`

A27. Show that if you apply two successive shift transformations and they share the same alphabet then the result is also a shift transformation. Is the result true if you replace the word "shift" is replaced by "affine" in the sentence above ? Show, using an example, that the sentence is not true if the second alphabet is a superset of the first.

A28. If the affine transform used is $x' \equiv 146x + 671 \bmod 729$ what relationship do we use to restore any message so coded ? Is there any digraph which is mapped to itself using the transform ?

A29. Evaluate $\tau(n)$, $\sigma(n)$ and $\phi(n)$ for $n = 22, \ldots, 28$ by finding the divisors of n.

A30. Evaluate $\tau(n)$, $\sigma(n)$ and $\phi(n)$ for $n = 121, \ldots, 129$ using the product formulae.

A31. Which numbers have $\tau(n) = 4$, $\sigma(n) = 42$, $\phi(n) = 12$?

A32. Show there are an infinite number of n for which $\tau(n) = k$ for any $k \in \mathbb{Z}$ and that $\sigma(n) = k$ always has only a finite number of solutions.

A33. Show that if $f(n)$ is a multiplicative function then so is $g(n) := \frac{f(n)}{n}$.

A34. Verify Wilson's theorem for $p = 2, 3, 5, 7, 11$. What is the case for the other numbers less than 11 ? Prove a theorem based on this evidence.

A35. Verify directly that $6^{12} \equiv 1 \bmod 13$ using reduction modulo 13.

A36. Construct the table of inverses for modulus 17 and hence solve $10x \equiv 3 \bmod 17$ and $8x + 3 \equiv 11x - 7 \bmod 17$.

A37. What is $\phi(11)$? Hence find the primitive roots of 11.
Make a table of indices for 11 and hence solve

$$x^2 + 4x \equiv 3 \bmod 11 \quad , \quad x^2 \equiv 2x \bmod 11, \qquad x^7 \equiv 3 \bmod 11$$
$$7x^3 \equiv 9 \bmod 11 \qquad \text{and} \qquad 5^x \equiv 8 \bmod 11$$

Repeat your calculations with a different primitive root of 11.

A38. Find the orders of the residues mod 23. Which are primitive roots ?

A39. Using the method described in the notes show that 131 071 (=$2^{17} - 1$) is prime.

A40. Prove that if q and p are odd primes and $q|(a^p + 1)$ then $q|(a + 1)$ or $q = 2kp + 1$ for some integer k. Hence show that 174 763 is prime.

A41. Show that $2^{19} - 1$ is a Mersenne prime.

A42. Determine the values of the following Legendre symbols:

$$\left(\frac{65}{577}\right) \qquad \left(\frac{513}{811}\right) \qquad \left(\frac{132}{541}\right) \qquad \left(\frac{11543}{13003}\right)$$

A43. Which primes p satisfy $\left(\frac{6}{p}\right) = 1$?

A44. Find the primes for which 6 is a quadratic residue and those for which -6 is a quadratic non-residue.

A45. Show that if n has the base 10 representation $d_1 d_2 \ldots d_k$ then the following statements hold:

(a) $3|n$ if and only if $\sum_{i=1}^{k} d_i \equiv 0 \bmod 3$.

(b) $7|n$ if and only if $d_k + 3d_{k-1} + 2d_{k-2} + d_{k-3} + 3d_{k-4} + 2d_{k-5} + \cdots \equiv 0 \bmod 7$.

(c) $9|n$ if and only if $\sum_{i=1}^{k} d_i \equiv 0 \bmod 9$.

Find and prove similar rules for $2|n$, $4|n$, $5|n$ and $11|n$.

A46. Using base 12 evaluate these problems:

$$\begin{array}{r} 3\delta108 \\ +66717 \end{array} \qquad \begin{array}{r} 54\varepsilon \\ \times 29 \end{array} \qquad \frac{911}{25}$$

A47. In base 12 again, construct similar rules to those in question A45.

A48. Make up a multiplication table in base 5 and find all of the primes between 300 and 444 working throughout in that base.

A49. A *Palindromic Number* is one which reads the same forwards as backwards. Prove that every 2 or 4-digit palindromic number is divisible by 11. Is this true for any even-digit palindromic number ? What if it has an odd number of digits? What can you prove similarly about palindromic numbers in base 12?

A50. What are the continued fraction representations of these numbers?

$$\frac{55}{41} \qquad \sqrt{11} \qquad \frac{\sqrt{7}-2}{5}$$

A51. What are the rational values of these continued fractions ?

$$(0,4,7) \qquad (5,2,2) \qquad (0,1,2,3)$$

A52. What are the surd values of these continued fractions ?

$$(3,\overline{4}) \qquad (2,\overline{1,2}) \qquad (0,1,2,\overline{6,3})$$

A53. Find a solution to the equation $x^2 - 13y^2 = 1$.

A54. Factorise $10^{11} - 1$ using all of the methods learnt in the course. Which is the fastest method in this case?

END OF QUESTION PAPER