UNSW AUSTRALIA.

SCHOOL OF MATHEMATICS AND STATISTICS MATH5645 TOPICS IN NUMBER THEORY

1. SOME CLASSICAL NUMBER THEORY:

1 Find all positive integers n such that
a. $\phi(n) = 12$ **b.** $\phi(2n) = \phi(n)$ and show that $\phi(n) = 14$ is impossible.

2 Suppose m and n are relatively prime positive integers, show that

$$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \bmod mn.$$

3 Show that $\phi(n) = n \prod_{\substack{p|n \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right)$.

4 Prove that

$$\sum_{(x,n)=1} x = \frac{1}{2} n\phi(n), \qquad (1 \le x \le n).$$

(**Hint:** If $\mathbb{U}_n = \{x_1, x_2, \ldots, x_{\phi(n)}\}$ then $\mathbb{U}_n$ can also be written as $\{n - x_1, \ldots, n - x_{\phi(n)}\}$.)

5 How many fractions $\frac{r}{s}$ are there satisfying $(r, s) = 1$ and $0 < r < s \le n$?

6 **a.** If g is a primitive root modulo p, an odd prime, show that $h = g^k$, where $(k, p-1) = 1$, is also a primitive root.
b. Compute all primitive roots for $p = 13$, and $p = 17$.

7 Consider a prime p of the form $4t + 1$. Show that a is a primitive root modulo p iff $-a$ is a primitive root mod p.

8 **a.** Find the number of primitive roots in $\mathbb{Z}_{13}$, $\mathbb{Z}_{101}$, $\mathbb{Z}_{12}$.
b. If $q = 2^{2^p} + 1$ is a prime show that $\mathbb{Z}_q$ has $2^{2^p - 1}$ primitive roots.

9 **a.** Use the existence of a primitive root modulo p to prove Wilson's Theorem.
b. Suppose p is prime. Prove that $1^k + 2^k + \cdots + (p-1)^k \equiv 0 \bmod p$ if $(p-1) \not| k$
[The converse, which would conclude the primality of p from this congruence, is an unsolved problem.]

10 If a has order 3 mod p, p a prime greater than 5, show that $(1 + a)$ has order 6.

11 Suppose p is prime and $p \equiv 1 \bmod 4$. Prove that the product of the quadratic residues mod p is -1. What if $p \equiv 3 \bmod 4$?

12 Show that for p prime, the set of quadratic residues mod p forms a subgroup of $\mathbb{U}_p$.

13 Suppose q and $p = 4q + 1$ are **both** prime. Prove that $2^{2q} \equiv -1 \bmod p$ and deduce that 2 is a primitive root mod p. (Hint: $p \equiv 5 \bmod 8$. What does this tell us about the number 2 in $\mathbb{Z}_p$?)

14 Suppose $p \equiv 3 \bmod 4$ and $q = 2p + 1$ are **both** prime.
a. Show that $\left(\frac{2}{q}\right) = 1$.
b. Use Euler's criterion to deduce that $2^p \equiv 1 \bmod q$.
c. Find a prime factor of $2^{251} - 1$.

15 **a.** Explain why every primitive root modulo a prime p must also be a quadratic non-residue.
b. How many quadratic non-residues in $\mathbb{Z}_{47}$ are not primitive roots? Can you find them?

16 If p and $q = 2p + 1$ are both odd primes, show that -4 and $2(-1)^{\frac{p-1}{2}}$ are both primitive roots modulo q.

17 Evaluate $\left(\dfrac{666}{2137}\right), \left(\dfrac{1001}{19991}\right)$ (Note that 19991 and 2137 are both primes.)

18 Evaluate $\left(\dfrac{-31}{127}\right)$, and hence prove that $127x^2 - y^2 = 31$ has no integer solutions.

19 Prove the following, ($q.r. \equiv$ quadratic residue, p is a prime).
a. -2 is a q.r. iff $p \equiv 1, 3 \bmod 8$ **b.** 3 is a q.r. iff $p = 12n \pm 1$
c. 5 is a q.r. iff $p = 10n \pm 1$ **d.** 6 is q.r. iff $p \equiv 1, -1, 5, -5 \bmod 24$.

20 Show that if -3 is a quadratic residue modulo a prime p, then $p \equiv 1 \bmod 6$.

21 A triangular number has the form $\dfrac{1}{2}n(n+1)$. Prove that if m is the sum of 2 triangular numbers then $4m+1$ is the sum of two squares.

22 Show that 21 is not the sum of two **rational** squares.

23 Let p be an odd prime. Show that if p can be represented in the form $p = x^2 + 2y^2$ then $p \equiv 1$ or 3 mod 8.

24 Find all right triangles with sides of integral length such that one leg differs by 2 from the hypotenuse.

25 If $a^2 + b^2 = c^2$ when a, b, c integers, show that abc is a multiple of 60.

26 **a.** If a, b are both even or both odd what can you say about $a + b$ and $a - b$?
b. If $\left(\dfrac{a+b}{2}\right)^2 + \left(\dfrac{a-b}{2}\right)^2 + \left(\dfrac{c+d}{2}\right)^2 + \left(\dfrac{c-d}{2}\right)^2 = k(a^2 + b^2 + c^2 + d^2)$ find k.
c. Given $1^2 + 3^2 + 5^2 + 7^2 = 84$ express 42 as the sum of 4 squares.

27 Show that a number of the form $16n - 1$ cannot be expressed as the sum of fewer than 15 fourth powers.

BRIEF SOLUTIONS

1 **a.** 28, 21, 42, 36, 13, 26 **b.** n is any odd number. **5** $\sum_{k=2}^{n} \phi(k)$.

6 $\pm 2, \pm 6; \pm 3, \pm 5, \pm 6, \pm 7$. **8** **a.** 4,40, none **14** **c.** 503

15 There is only one, namely -1. **17** $1, -1$.

24 $(k^2-1, 2k, k^2+1)$, or $(2k-2, 4k^2-4k, 4k^2-4k+2)$, where k is a positive integer greater than 1.

26 **c.** $1^2+2^2+6^2+1^2$.
