ASSIGNMENT 1

1. Use mathematical induction to show that the sum of the cubes of three consecutive non-negative integers is divisible by 9.

2. (i) If $d \mid a$ and $d \mid b$, prove that $d \mid (a+b)$.

   (ii) More generally, if $d \mid a$ and $d \mid b$, prove that $d \mid (xa+yb)$ for any integers x and y.

3. Let $d = (a, b)$ and suppose that x and y are integers such that $xa + yb = m$.

   (a) What is the relationship between d and m?

   (b) If $m = 1$, show that $d = 1$.

   (c) Suppose that $xa + yb = 6$. What are the possible values of (a, b)?

   (**Note:** (b) is a very useful special case. When $m > 1$, we cannot conclude that $m = d$.)

4. Find the gcd of 212 and 153 and express it in the form $212x + 153y$.

5. Find the prime factorisations of each of the following integers.
   (a) 126, (b) 2222220.

6. (a) Suppose that in the prime factorisation of n, only even powers of primes occur. Show that n is a perfect square, i.e., $n = m^2$ for some integer m.

   (b) Find the prime factorisation or 324, and from it write down the prime factorisation of $\sqrt{324}$.

7. If $(a, b) = 1$, $a \mid c$ and $b \mid c$, show that $ab \mid c$. Give an example to show that the result need not be true when $(a, b) \neq 1$.

8. Show that if a, b, and c are integers with $(a, b) = (a, c) = 1$, then $(a, bc) = 1$.

9. (a) Show that the product of two integers of the form $6k + 1$ is of the form $6k + 1$.

   (b) Prove that there are infinitely many primes of the form $6k + 5$, where k is a positive integer.

   Hint: Suppose there are only finitely many primes of the form $6n + 5$ and list them as $p_0, p_1, p_2, \ldots, p_r$ where $p_0 = 5, p_1 = 11, p_2 = 17, \ldots$. Let $Q = 6p_1p_2 \cdots p_r + 5$, and consider the prime factorisation of Q.

10. A student returning from Europe changes her French francs and Austrian schillings into Australian money. If she receives \$16.84 and has received 25c for each French franc and 12c for each Austrian schilling, what amounts of each type of currency did she exchange, given that she started with at least

35 of each?
(*Set the problem up as a linear Diophantine equation and use the methods of this section*).

11. Use Fermat's method to factorise 38021.

ASSIGNMENT 2

1. Solve the following linear congruences (you may if you wish, find some solutions by inspection):
   (a) $3x \equiv 9 \pmod{14}$, (b) $3x \equiv 5 \pmod{7}$,
   (c) $4x \equiv 5 \pmod{6}$, (d) $4x \equiv 8 \pmod{12}$.

2. Solve $153x \equiv 11 \pmod{212}$.
   (**Hint:** You may find the calculation you did in Assignment 1 Question 4 useful).

3. Use congruences to verify the divisibility statement $13 \mid (145^6 + 1)$.

4. Solve $x^3 + x + 1 \equiv 0 \pmod{3}$ using any method you wish.

5. Show that if a is an odd integer, then $a^2 \equiv 1 \pmod{8}$.

6. Find an inverse modulo 23 of each of the following integers.
   (a) 4, (b) 6, (c) 10.

7. In the ISBN of a book the fourth digit is unreadable, so the number is 3-76?3-5197-7. Recover the missing digit knowing that $\sum_{k=1}^{10} kx_k \equiv 0 \pmod{11}$ where x_k is the k-th digit of the ISBN.

8. If $(m, n) = 1$ and $m \geq 3, n \geq 3$, show that the congruence

   $$x^2 \equiv 1 \pmod{mn}$$

   has solutions other than $x \equiv \pm 1 \pmod{mn}$.

9. Solve the following ancient Indian problem: If eggs are removed from a basket two, three, four, five, and six at a time, there remain, respectively, one, two, three, four, and five eggs. But if the eggs are removed seven at a time no eggs remain. What is the least number of eggs that could have been in the basket? (**Hint:** You may find it useful to first solve the problem formed by the last three conditions).

10. Prove that a number n is divisible by 7 if and only if $n' - 2n_0$ is divisible by 7 where n_0 is the last digit and n' is the number obtained from n by deleting the last digit. (**Hint:** Prove that $-2n \equiv n' - 2n_0 \bmod 7$).

11. Set up a round-robin tournament schedule for (a) 7 teams, (b) 8 teams.

12. Assume $\{r_1, \ldots, r_n\}$ is a complete system modulo n. Show that, for any integer a, the set $\{r_1 + a, \ldots, r_n + a\}$ is also a complete system.

ASSIGNMENT 3

1. Illustrate the proof of Wilson's Theorem with $p = 13$.

2. Using Fermat's Little Theorem, find the remainder when $2^{100,000}$ is divided by 13.

3. Using Euler's Theorem, find the remainder when $5^{100,000}$ is divided by 18.

4. Show that if n is odd and 3 does not divide n, then $n^2 \equiv 1 \pmod{24}$.
(**Hint:** It may help to note that $24 = 3 \times 8$.)

5. Evaluate $\phi(n)$, $\tau(n)$ and $\sigma(n)$ for each n such that $25 \leq n \leq 30$.

6. Prove that if n is odd, then $\tau(n) \equiv \sigma(n) \pmod{2}$.

7. (a) If n is odd and $(n, 5) = 1$, show that $5 \mid (n^4 + 4^n)$.

   (b) For which positive integers n is $n^4 + 4^n$ prime?

   Hint for (b): Deal with the case n even first. For n odd, factorise $n^4 + 4^n$ as a product of two terms by completing squares (This is a hard problem!).

8. Find the primes p and q if $n = pq = 14647$ and $\phi(n) = 14400$.

9. What is the ciphertext that is produced when the RSA cipher with key $e = 3$, $n = 3763$ is used to encipher the message GO?

10. The next meeting of cryptographers will be held in the town of 2173 1584 . It is known that the cipher-text in this message was produced using the RSA cipher key $e = 1997$, $n = 2669$. Where will the meeting be held?

11. One of the oldest recorded cipher systems is the Caesar cipher, obtained by using a cyclic shift of the letters of the alphabet. It is rather primitive compared to the RSA system, and is easily broken. The following message was sent using this code. Decipher the message, given that e is the most common letter in English.

QJY YMJR JFY HFPJ

ASSIGNMENT 4

1. (a) Find the order of the integers 2, 3 and 5 modulo 13.

   (b) Find the order of the integers 2, 3 and 5 modulo19.

2. Find a primitive root for each of 13 and 19.

3. Find the order of the integers 1, 3, 7, and 9 modulo 10. Which of these numbers are primitive roots modulo 10?

4. Show that if a is an integer relatively prime to the positive integer m and $\text{ord}_m a = st$, then $\text{ord}_m a^t = s$.

5. (a) Show that the odd prime divisors of the integer $n^2 + 1$ are of the form $4k + 1$. (**Hint:** If p is an odd prime which divides $n^2 + 1$, show that n has order 4 modulo p).

   (b) Show that the odd prime divisors of the integer $n^4 + 1$ are of the form $8k + 1$. (**Hint:** If p is an odd prime which divides $n^4 + 1$, show that n has order 8 modulo p).

6. Show that if p is a prime and $p \equiv 1 \pmod 4$, there is an integer x such that $x^2 \equiv -1 \pmod p$. (**Hint:** Use theory to show that there is an integer x of order 4 modulo p.)

7. How many primitive roots are there for the prime 97?

8. Given that 5 is a primitive root for 23, express all the other primitive roots of 23 as powers of 5.

9. Write out a table of indices modulo 23 with respect to the primitive root 5.

10. (a) Find all the solutions of the congruence $3x^5 \equiv 1 \pmod{23}$.

    (b) Find all the solutions of the congruence $13^x \equiv 5 \pmod{23}$.

11. (Review question). Let a and b be non-zero integers. Which of the following are correct definitions of '$a \mid b$'?

    (a) '$b = ax$ for some x'

    (b) '$b = ax$ for some integer x'

    (c) '$a = bx$ for some x'

    (d) '$b = ax$ for every integer x'

    (e) 'There exists an integer x such that $b = ax$'

    (f) '$b = ax$'.

ASSIGNMENT 5

1. Find all the quadratic residues and non-residues of 17.

2. Let p be prime and a a quadratic residue of p. Show that if $p \equiv 1 \pmod 4$, then $-a$ is also a quadratic residue of p, while if $p \equiv 3 \pmod 4$, then $-a$ is a quadratic nonresidue of p.

3. Evaluate each of the following Legendre symbols:

$$\text{(a) } \left(\frac{19}{23}\right), \text{ (b) } \left(\frac{17}{79}\right), \text{ (c) } \left(\frac{18}{101}\right).$$

4. Show that if p is an odd prime, then

$$\begin{aligned} \left(\frac{-3}{p}\right) &= 1 \text{ if } p \equiv 1 \pmod 3, \\ \left(\frac{-3}{p}\right) &= -1 \text{ if } p \equiv -1 \pmod 3. \end{aligned}$$

5. Evaluate the Jacobi symbol

$$\left(\frac{22}{35}\right)$$

6. Show that the integer 561 is an Euler pseudoprime to the base 2.

7. Show that if n is an Euler pseudoprime to the bases a and b, then n is an Euler pseudoprime to the base ab.

ASSIGNMENT 6

1. Find all primitive Pythagorean triples, x, y, z with $z \leq 13$.

2. Find all Pythagorean triples x, y, z, not necessarily primitive, in which $z = 50$.

3. Let x, y, z be a primitive Pythagorean triple (with y even). Show

   (i) $z \equiv 1 \pmod 4$.

   (ii) y is divisible by 4.

   (iii) Exactly one of x, y is divisible by 3.

   (iv) Exactly one of x, y, z is divisible by 5.

   Deduce that xyz is divisible by 60.

4. Find a Pythagorean triple x, y, z (with y even) which cannot be written in the form

$$\begin{aligned} x &= m^2 - n^2, \\ y &= 2mn, \\ z &= m^2 + n^2, \end{aligned}$$

   with m, n integers. (Such an example will of course have to be non-primitive.)

5. Find all solutions in positive integers of the diophantine equation

$$x^2 + 2y^2 = z^2.$$

6. Let p be prime. Using Fermat's little theorem, show that

   (a) if $x^{p-1} + y^{p-1} = z^{p-1}$, then $p \mid xyz$.

   (b) if $x^p + y^p = z^p$, then $p \mid (x + y - z)$.

7. Show that the diophantine equation $x^4 - y^4 = z^2$ has no solutions in nonzero integers. (**Hint:** Try the same method as used on $x^4 + y^4 = z^2$. The problem is hard.)