MA3H1 Topics in Number Theory
Some Homework Hints

Important Health Warning: Make sure you have tried to do the homework questions on your own before reading the hints.

Sheet 2, Question 5.

(a) Suppose m is not a power of 2. Write $m = 2^n a$ where a is odd. Then $a > 1$. Let $X = 2^{2^n}$. Then $2^m + 1 = X^a + 1$. Now you should be able to show that $2^m + 1$ is composite using the identity

$$X^a + 1 = (X+1)(X^{a-1} - X^{a-2} + X^{a-3} - X^{a-4} + \cdots + 1).$$

(b) Suppose $b > a$. Note that

$$2^{2^a} \equiv -1 \pmod{F_a},$$

so

$$2^{2^b} = \left(2^{2^a}\right)^{2^{b-a}} \equiv 1 \pmod{F_a}.$$

Adding 1 to both sides gives

$$F_b \equiv 2 \pmod{F_a}.$$

In other words, $F_b - 2 = kF_a$ where k is some integer. Let $g = \gcd(F_a, F_b)$. Then g divides 2 as it divides both F_a and F_b. But g is also odd as F_a is odd. So $g = 1$.

(c) Suppose $p \mid F_n$ where p is a prime. Since $F_n \equiv 0 \pmod{p}$ we have

$$2^{2^n} \equiv -1 \pmod{p}.$$

Squaring we get

$$2^{2^{n+1}} \equiv 1 \pmod{p}.$$

Let d be the order of 2 modulo p. By Theorem 2.4 (part (i)) in the notes we have that $d \mid 2^{n+1}$. We will show that $d = 2^{n+1}$. Suppose it isn't. Then $d = 2^k$ for some $k \le n$. Now

$$2^{2^k} = 2^d \equiv 1 \pmod{p}$$

by the definition of order. Raising both sides to 2^{n-k} we obtain

$$2^{2^n} = \left(2^{2^k}\right)^{2^{n-k}} \equiv 1 \pmod{p}$$

which contradicts the above congruence $2^{2^n} \equiv -1 \pmod{p}$. Hence $d = 2^{n+1}$. Now by part (ii) of Theorem 2.4 in the notes, $2^{n+1} = d$ divides $\varphi(p) = p - 1$.

(d) Fix n. Let $m \ge n$ and let p_m be a prime divisor of F_m. By part (c), we have $2^{m+1} \mid (p_m - 1)$. However, as $n \le m$ we have $2^n \mid (p_m - 1)$ so $p_m \equiv 1 \pmod{2^n}$. In other words, for each $m \ge n$, we have a prime $p_m \equiv 1 \pmod{2^n}$. Are they infinitely many? They are if they are distinct. However if $m_1 \ne m_2$ then p_{m_1} divides F_{m_1} and p_{m_2} divides F_{m_2}. By part (b), F_{m_1} and F_{m_2} are coprime, so $p_{m_1} \ne p_{m_2}$, so indeed we get infinitely many primes $\equiv 1 \pmod{2^n}$.

Sheet 2, Question 6.

(b) We use part (a) to help us count the squares mod p. The numbers mod p are just $0, 1, 2, \ldots, p-1$. So the squares mod p are $0^2, 1^2, \ldots, (p-1)^2$. Thus it looks like there should be p squares. However, the list has repetition in it, so we have to take account of the repetition. Let x, y be among $0, \ldots, p-1$ such that $x^2 \equiv y^2 \pmod{p}$. By (a) we know that $x \equiv \pm y \pmod{p}$. If $x = 0$ then $y \equiv 0$ and so $y = 0$ (as it is one of $0, \ldots, p-1$) so 0^2 is not repeated. If $1 \le x \le p-1$, then $y = x$ of $y = p - x$ (this is the only way we can have $x \equiv \pm y \pmod{p}$ among $1, 2, \ldots, p-1$). Thus the squares mod p are really $0^2, 1^2, \ldots, ((p-1)/2)^2$. This is exactly $(p-1)/2 + 1 = (p+1)/2$ numbers.

To understand part (b) it might help to write down some examples. E.g. square all the numbers mod 7 and see the repetition.

(c) There are $(p+1)/2$ numbers of the form x^2 mod p. There are $(p+1)/2$ numbers of the form $-1 - y^2$ mod p (because to get the numbers of the form $-1 - y^2$, multiply the squares by -1 and subtract 1—this will not change how many they are). There are exactly p numbers mod p. Note that $(p+1)/2$ is more than half of p. So the set of numbers of the form x^2 and those of the form $(p+1)/2$ must have at least one common element (if not, we will have too many distinct numbers mod p). So there are some x and y such that $x^2 \equiv -1 - y^2 \pmod{p}$. In otherwords, $x^2 + y^2 + 1 \equiv 0 \pmod{p}$.

(d) Since m is squarefree, we can write $m = p_1 p_2 \ldots p_r$ where the p_i are distinct primes. By part (c), for each i there are integers x_i, y_i such that

$$x_i^2 + y_i^2 + 1 \equiv 0 \pmod{p_i}.$$

By the Chinese Remainder Theorem, there is an integer x such that

$$x \equiv x_i \pmod{p_i},$$

and likewise an integer y such that

$$y \equiv y_i \pmod{p_i}.$$

Now

$$x^2 + y^2 + 1 \equiv x_i^2 + y_i^2 + 1 \equiv 0 \pmod{p_i}.$$

Hence $p_i \mid (x^2+y^2+1)$ for $i = 1, \ldots, r$. Since the p_i are distinct primes, $m \mid (x^2+y^2+1)$. Thus

$$x^2 + y^2 + 1 \equiv 0 \pmod{m}.$$

Sheet 3, Question 3

Part (iii). We want to solve $3^m - 2^n = 1$. Suppose first that $n \ge 3$. Then $8 \mid 2^n$. Thus $2^n \equiv 0 \pmod{8}$ and so $3^m \equiv 1 \pmod{8}$. Using part (ii) we have that m is even, so we can write $m = 2k$ with k a non-negative integer. Therefore,

$$(3^k - 1)(3^k + 1) = 2^n.$$

So, $3^k - 1 = 2^a$ and $3^k + 1 = 2^b$ where a and b are positive integers. Subtracting we get

$$2 = 2^b - 2^a.$$

The only powers of 2 that differ by 2 are 2^2 and 2^1, so $b = 2$ and $a = 1$. In this case $k = 1$ and $m = 2$ and we get that $n = 3$. Now suppose $n < 3$. Then $n = 0, 1, 2$. Trying all the possibilities in $3^m = 2^n + 1$ gives us $n = 1$ and $m = 1$. So the only solutions are $(m, n) = (1, 1)$ and $(2, 3)$.

Sheet 3, Question 6.

Let g be a primitive root modulo p. We know that the non-zero residues modulo p are

$$1, g, g^2, \dots, g^{p-2}.$$

By Lemma 3.1 in the notes, the ones with even exponent are the quadratic residues:

$$R = \{1, g^2, g^4, \dots, g^{p-3}\}$$

and the ones with the odd exponent are the quadratic non-residues:

$$N = \{g, g^3, g^5, \dots, g^{p-2}\}.$$

Thus the product of the quadratic residues is

$$\prod_{r \in R} r \equiv 1 \cdot g^2 \cdot g^4 \cdots g^{p-3} \equiv g^{0+2+\cdots+p-3} \pmod{p}.$$

Now

$$0 + 2 + \cdots + p - 3 = 2(1 + 2 + \cdots + (p-3)/2) = \frac{p-3}{2} \cdot \frac{p-1}{2},$$

by the formula for the arithmetic progression. But

$$g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

as g is a quadratic non-residue (it's in the list of quadratic non-residues!)—here we used Euler's Criterion. Hence the product of quadratic residues is

$$\left(g^{\frac{p+1}{2}}\right)^{\frac{p-3}{2}} \equiv (-1)^{\frac{p-3}{2}} = (-1)^{\frac{p+1}{2}} \pmod{p},$$

since

$$\frac{p-1}{2} = 2 + \frac{p-3}{2}.$$

The product of the quadratic non-residues is similar. For part (ii), you need to use the formula for the geometric progression. After a couple of steps you will get:

$$\sum_{r \in R} r \equiv 1 + g^2 + \cdots + g^{p-3} = \frac{g^{p-1} - 1}{g^2 - 1} \pmod{p}.$$

Now by Fermat's Little Theorem, the numerator $\equiv 0 \pmod{p}$, and so $\sum r \in Rr \equiv 0 \pmod{p}$. However, before this makes sense, you must check that $g^2 \not\equiv 1 \pmod{p}$. This true since g is a primitive root and its order is $p - 1 > 2$ as long as $p > 3$. The question assumes that $p > 3$ so everything is fine.

Sheet 4, Question 5.

(i) We're given that p, q are primes and $p = 2q + 1$. Also $q \equiv 1 \pmod{4}$. We must show that 2 is a primitive root modulo p. We know that the order of 2 divides $p - 1 = 2q$. We must show that the order of 2 modulo p equals $p - 1$. Now the order can by 1, 2, q and $2q = p - 1$. We must exclude the first three possibilities. Suppose the order is 1. Then this means that $2^1 \equiv 1 \pmod{p}$ and so $p \mid 1$ which is impossible. Similarly we can rule out that the order is 2. Suppose the order is $q = (p-1)/2$. Then

$$2^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

and so by Euler's criterion

$$\left(\frac{2}{p}\right) = 1.$$

It follows that $p \equiv 1, 7 \pmod 8$ by the supplement to the Law of Quadratic Reciprocity. But $q \equiv 1 \pmod 4$ so $q = 1 + 4n$ where n is an integer, so $p = 2q + 1 = 3 + 8n \equiv 3 \pmod 8$ giving a contradiction.

(ii) You have to think about the order of 5 modulo p. Note that $p = 2q + 1$ so $p - 1 = 2q$. The order of 5 modulo p divides $2q$. So it is either 1 or 2 or q or $2q$. To prove that 5 is a primitive root you must prove that 5 has order $2q$. Now if 5 has order 1 then 5 is congruent to 1 modulo p and so p divides 4, so $p = 2$. If 5 has order 2 modulo p then $5^2 = 25$ is congruent to 1 modulo p and so p divides 24, so $p = 2$ or 3.

But as $p = 2q + 1$, and q is prime, p is not 2 and not 3. So the order of 5 modulo p is not 1 and not 2. So it must be q or $2q$. If 5 is a quadratic residue then the order is q and if 5 is not a quadratic residue then the order is $2q$. This you get from Euler's Criterion This should help you to complete the question.

Sheet 4, Question 6. This is similar to the proof of Theorem 3.6.

Sheet 5, Question 5.

We are told that $p \equiv 1 \pmod 3$. Let g be a primitive root from p; thus g has exact order $p - 1$. Let $f = g^{(p-1)/3}$. Then f has exact order 3. So $f \not\equiv 1 \pmod p$ but $f^3 \equiv 1 \pmod p$. Now $f^3 - 1 \equiv 0 \pmod p$. Factoring we obtain

$$(f - 1)(f^2 + f + 1) \equiv 0 \pmod p$$

and we know that $f - 1 \not\equiv 0 \pmod p$. Hence $f^2 + f + 1 \equiv 0 \pmod p$.

Now take

$$S = \{(x, y) \in \mathbb{R}^2 : x^2 + xy + y^2 < 2p\}$$

and $\Lambda = \{(x, y) \in \mathbb{Z}^2 : x \equiv fy \pmod p\}$ and apply Minkowski's Theorem. To see that S is an ellipse and calculate its area we complete the square:

$$(x + y/2)^2 + 3y^2/4 < 2p.$$

For the moment, let $u = x + y/2$ and $v = y$. Then, with this change of variable S becomes

$$S' = \{(u, v) \in \mathbb{R}^2 : u^2 + 3v^2/4 < 2p\}.$$

You can apply the formula for the area of the ellipse to obtain the area of S'. What is the relation between the area of S and the area of S'? To get that you need to calculate the Jacobian of change of variable:

$$\frac{\partial(u, v)}{\partial(x, y)} = \begin{vmatrix} \frac{\partial u}{\partial x} & \frac{\partial u}{\partial y} \\ \frac{\partial v}{\partial x} & \frac{\partial v}{\partial y} \end{vmatrix} = 1.$$

Hence

$$\text{Area of } S = \iint_S dxdy = \iint_{S'} dudv = \text{Area of } S'.$$