2.4.1 Let \( m = qn + r \) with \( 0 \leq r < n \) and \( |g| = n \). We have \( g^m = g^{qn+r} = (g^n)^q \cdot g^r = e^q \cdot g^r \). Since \( 0 \leq r < |g| \) it follows that \( r = 0 \) i.e. \( n \) divides \( m \).

2.4.2 \( \{\mathbb{Z}/13\mathbb{Z}\}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}, \{5\} = \{5, 11\}, \{6\} = \{6, 7\}, \{7\} = \{7\} \) since \( 5^4 = 1 \) modulo 13. Note that \( 2 < 5 \Rightarrow \{2\} \), 5 and \( 4 < 5 \Rightarrow \{4\} \) We then have \( \{\mathbb{Z}/13\mathbb{Z}\}^* = \{5\} \) is the disjoint union of the three equivalence classes each of size 4 i.e. 12 = 3 · 4.

2.5.1 By the FTA we have \( mx + ny = 1 \) and by assumption \( a = mk \) and \( a = nj \). Therefore \( k = k + nk = ax + kny = n(1 + ny) \), thus \( a = mk = mn(1 + ny) \) and \( mn \) divides \( a \).

2.5.2 \( 1000 = 2^35^4 \) and so the divisors of 1000 are 1, 2, 4, 8, 5, 10, 20, 40, 25, 50, 100, 200, 125, 250, 500, 1000. We have \( \varphi(1) = 1 \), \( \varphi(2) = 1 \), \( \varphi(4) = 2 \), \( \varphi(8) = 4 \), \( \varphi(5) = 4 \), \( \varphi(10) = 4 \), \( \varphi(20) = 8 \), \( \varphi(40) = 16 \), \( \varphi(25) = 20 \), \( \varphi(50) = 20 \), \( \varphi(100) = 40 \), \( \varphi(200) = 80 \), \( \varphi(125) = 100 \), \( \varphi(250) = 100 \), \( \varphi(500) = 200 \), \( \varphi(1000) = 400 \). Finally \( 1 + 2 + 4 + 4 + 8 + 8 + 16 + 20 + 20 + 40 + 80 + 100 + 100 + 200 + 400 = 1000 \).

2.5.3 \( x \equiv_{11} 5 \) implies \( x = 5 + 11k \) and so \( 5 + 11k \equiv_{13} 7 \) i.e. \( 11k \equiv_{13} 2 \). The inverse of 11 modulo 13 is 6 (6 · 11 − 5 · 13 = 1) so \( k \equiv_{13} 6 \cdot 11 \cdot k \equiv_{13} 6 \cdot 2 \equiv_{13} 12 \). Finally \( x = 5 + 11 \cdot 12 = 137 \).

2.5.4 \( x \equiv_{16} 11 \) implies \( x = 11 + 16k \) and so \( 11 + 16k \equiv_{27} 16 \) i.e. \( 16k \equiv_{27} 5 \). The inverse of 16 modulo 27 is \( -5 (=-5 \cdot 16 \cdot 3 \cdot 27 = 1) \) so \( k \equiv_{27} -5 \cdot 16 \cdot k \equiv_{27} -5 \cdot 5 \equiv_{27} -25 \equiv_{27} 2 \). Finally \( x = 11 + 2 \cdot 16 = 43 \).

2.5.5 We compute the last two digits of powers of two (i.e. \( 2^i \) modulo 100). \( 2^0 = 1 \), \( 2^1 = 2 \), \( 2^2 = 4 \), \( 2^4 = 16 \), \( 2^8 = 162 \), \( 2^{16} = 256 \), \( 2^{32} = 512 \), \( 2^{64} = 96 \), \( 2^{128} = 128 \), \( 2^{256} = 256 \), \( 2^{512} = 512 \), \( 2^{1024} = 512 \), \( 2^{2048} = 128 \), \( 2^{4096} = 128 \), \( 2^{8192} = 128 \). Since \( 9999 = 8192 + 1024 + 512 + 256 + 8 + 4 + 2 + 1 \), it follows that \( 2^{9999} = 2^{8192} \cdot 2^{1024} \cdot 2^{512} \cdot 2^{256} \cdot 2^{128} \cdot 2^{64} \cdot 2^{32} \cdot 2^{16} \cdot 2^{8} \cdot 2^{4} \cdot 2^{2} \cdot 2^{1} \approx 96 \cdot 16 \cdot 96 \cdot 36 \cdot 8 \cdot 16 \cdot 36 \cdot 8 = 16 \cdot 36 \cdot 36 \cdot 8 = 96 \cdot 16 \cdot 8 = 96 \cdot 16 \cdot 8 = 96 \cdot 16 \cdot 8 = 96 \cdot 16 \cdot 8 = 96 \cdot 16 \cdot 8 \).

4.1.2 Hint: \( f(x) \cdot 2 x = x^2 \). \( f(x) \cdot 2 x = \int f(-x) \cdot \frac{\sin(kx)}{k} dx \) and integrating by parts \( f(x) \cdot \frac{\sin(kx)}{k} dx = \frac{1}{2} \cdot \cos(kx) - \int \frac{-\cos(kx)}{k} dx \) but \( \int \frac{-\cos(kx)}{k} dx = 0 \) and \( \frac{1}{2} \cdot \cos(kx) = \frac{1}{2} \cdot \cos(kx) \).

4.2.1 Define \( \varepsilon(n) = 0, 1, 0, -1 \) if \( n \equiv_{4} 0, 1, 2, 3 \) and let

\[
L = \sum_{n \geq 1} \left( \frac{\varepsilon(n)}{n} \right) = \prod_{p \text{ prime}} \left( \sum_{i \geq 0} \left( \frac{\varepsilon(p)}{p} \right)^i \right)
\]

\[
= \prod_{p \equiv_{4} 1} \left( 1 + \frac{1}{p} + \frac{1}{p^2} + \ldots \right) \prod_{p \equiv_{4} 3} \left( 1 - \frac{1}{p} + \frac{1}{p^2} + \ldots \right)
\]

If there are finitely many \( p \equiv_{4} 1 \), then this behaves like

\[
\prod_{p \text{ prime}} \left( 1 - \frac{1}{p} + \frac{1}{p^2} + \ldots \right) \prod_{p \equiv_{4} 3} \left( \frac{p}{p-1} \right) = 0.
\]

If there are finitely many \( p \equiv_{4} 3 \), then this behaves like

\[
\prod_{p \text{ prime}} \left( 1 + \frac{1}{p} + \frac{1}{p^2} + \ldots \right) \prod_{p \equiv_{4} 3} \left( \frac{p}{p-1} \right) = +\infty.
\]
The above argument is not correct because $L$ is not absolutely convergent. However, let $L(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$, then $L(s)$ is absolutely convergent for all $s > 1$ and taking the limit as $s \to 1$, the above argument becomes correct.

4.3.1 $\sigma(3^{2k+1}) = (3^{2k+2} - 1)/(3 - 1)$. Now $3^2 \equiv_k 1 \text{ so } 3^{2k+2} = (3^2)^{k+1} \equiv_k 1 \text{ so } 3^{2k+2} - 1$ is divisible by 8 so $3^{2k+2} - 1)/(3 - 1)$ is divisible by 4. So $\sigma(n) = \sigma(3^{2k+1})\sigma(r)$ is divisible by 4. But if $n$ is perfect, then $\sigma(n) = 2n$ so $\sigma(n)$ is not divisible by 4 (as $n$ is odd).

4.3.2 2047 = 23·89.

4.3.3 The number of digits is $\log(32.582.657 - 1)$ The number is about $\frac{32.582.657}{10} \log(2)$.

5.3.1 Let $\mu_n$ be the set of all $n$-th roots of 1 in $F^\times$. Clearly 1 $\in \mu_n$ so $\mu_n \neq \emptyset$. If $x,y \in \mu_n$, then by assumption $x^n = y^n = 1$. Now $(xy)^n = x^n y^n = 1 \cdot 1 = 1$ so that $\mu_n$ is closed under multiplication. Finally $(x^{-1})^n = (x^n)^{-1} = 1^{-1} = 1$ so that $\mu_n$ is closed under inverses and hence $\mu_n$ is a subgroup of $F$.

5.3.2 Taking the term of degree $n - 1$ in the equation

\[ x^n - 1 = (x - 1)(x - \zeta)(x - \zeta^2) \cdots (x - \zeta^{n-1}) \]

we obtain $0 = -1 - \zeta - \cdots - \zeta^{n-1}$.

5.3.3 The possible orders of 3 in $\mathbb{F}_{31}$ are the divisors of $|\mathbb{F}_{31}| = 30$ i.e. 1, 2, 3, 5, 6, 10, 15, 30. However 3^2 = 9, 3^3 = 27, 3^4 = 27 = 9 · (-4) = -36 = -5, 3^6 = -15, 3^10 = 25 and 3^15 = -125 = -1 are all $\neq 1$.

The 6-th roots of 1 are $3^0 = 1$, $3^1 = -5$, $3^{10} = 25$, $3^{15} = -1$, $3^{20} = 5$ and $3^{25} = 6$. Their sum is of course 0.

5.4.1 $I(7) + I(x) = I(5)$ (modulo 10) so 7 + I(x) = 4, so I(X) = -3 $\equiv_{10}$ 7 so $x = 2^7 = 7$.

5.4.2 $I(4) + 2I(x) = I(9)$ so 2 + 2I(x) = 6 so I(x) = 2 so $x = 2^2 = 4$.

5.4.3 $2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 16 = -3, 2^5 = -6 = 13, 2^6 = 7, 2^7 = 14,$

$2^8 = 9, 2^9 = 18 = -1, 2^{10} = -2 = 17, 2^{11} = -4 = 15, 2^{12} = -8 = 11, 2^{13} = -16 = 3, 2^{14} = 6, 2^{15} = 12, 2^{16} = 5, 2^{17} = 10, 2^{18} = 1.$

5I(x) = I(7) (modulo 18) so I(x) = -7 · 5 · I(x) = -7 · 6 = -42 $\equiv_{18}$ 12 so

$x = 2^{12} = 11.$

6.2.1 We have $6^2 = 36 = -5, 6^4 = 25, 6^8 = 625 = 10$ and $6^{16} = 1000 = 18$ so $6^{(p-1)/2} = 6^2 = 18 - 25 = 450 = 40 = -1.$ (But we knew this as $6^{20}$ is a square root of 1 so it is ±1, but it can’t be 1 as otherwise the order of 6 would be ≤ 20 but we assumed it is a primitive root i.e. it has order 40.)

6.2.2 $2^{(31-1)/2} = 2^15 = 32 = 1^3 = 1$ so 2 is a square mod 31. 315 = (27)^5 = (-4)^5 = -1 · 2^5 · 2^5 = -1 (as 2^5 = 32 = 1 mod 31). So 3 is not a square modulo 31.

$7^{(29-1)/2} = 7^4 = (20)^7 = (-4)^7 = -64 - 64 = -6 · 6 · 4 = -6 · 24 = -6 · (-5) = 30 = 1$ so 7 is a square modulo 29.

6.3.1 The order of 6 is 40, so the order of $g = 6^5$ is 8. Now, $g = 6^5 = 36 · 36 · 6 = (-5)^2 · 6 = 150 = 27$. We also have $g^2 = g^{-1} = -3$ (as 1 = 2 · 41 - 3 · 27). So $g + g^2 = 24$ is a square root of 2.

6.3.2 The order of 5 is 72 (in $\mathbb{F}_{72}$). So $g = 5^9$ has order 8. Now $g = 5^9 = (125)^3 = (-21)^3 = -441 · 21 = 3 · 21 = 63$. We have $g^7 = g^{-1} = -22$ (since 1 = 19 · 63 - 22 · 63). So $g + g^7 = 63 - 22 = 41$ is a square root of 2.

6.3.3 $g = 3 + 4 · 3 = 15 = -2$ is a primitive 8-th root of 1.

6.3.4 $x^2 - 6x + 11 = 0$ is equivalent to $(x - 3)^2 = -2$. We have $(\frac{-2}{11}) = (\frac{3}{11}) (\frac{-1}{11}).$

Since 131 $\equiv_k 3$, we have $(\frac{3}{131}) = -1$ and since 131 $\equiv_k 34$, we have $(\frac{131}{34}) = -1$.

Thus $(-1)^2 = 1$ and we can solve this equation.

8.1.1 $221 = 13 · 17 = (3^2 + 2^2)(4^2 + 2^2) = 14^2 + 5^2$. 
8.1.2 \(8^2 + 1^2 = 5 \cdot 13\). Pick 5/2 < u = -2, v = 1 ≤ 5/2 then \(xu + yv = -15\) and \(xv - yu = -10\). Dividing by -5 we get (3, 2) and \(3^2 + 2^2 = 13\).

8.1.3 Since 5 is a primitive root of 1 modulo 73, it has order 72, thus \((5^{18})^2 = 5^{36} \equiv 1 \pmod{73}\). We have \(5^3 = 125 \equiv 52, 5^4 \equiv 260 \equiv 41, 5^5 \equiv 205 \equiv -14, 5^6 \equiv -70 \equiv 3, 5^{18} \equiv 27\) and in fact \((27)^2 + 1^2 = 729 + 1 = 10 \cdot 73\). By descent, we pick 5 < u = -3, v = 1 ≤ 5 and so \(xu + yv = -80, xv - yu = 30\) and dividing by 10 we have \(8^2 + 3^2 = 64 + 9 = 73\).

\[\text{Math 4400, Fall 2014 Extra homework.}\]

3.2.3 Find the inverse of 1

3.2.7 Show that every element of \(F\)

3.2.8 Repeat 3.2.7 for

3.2.9 Explain why \(\mathbb{F}_3\) is contained in any field \(F\) of characteristic 3.

3.2.10 Explain why the solutions to \(x^6 + x^4 + x^2 + 1\) in \(\mathbb{F}_3[i]\) are exactly the elements of \(\mathbb{F}_3[i]\) \(\mathbb{F}_3\).

3.2.11 If \(a + bi \in \mathbb{F}_p[i]\) then let \(N(a + ib) = a^2 + b^2\). Show that \(N((a + ib)(c + id)) = N(a + ib)N(c + id)\) and deduce that \(a + bi \in \mathbb{F}_p[i]^*\) if and only if \(N(a + ib) \neq 0\).

4.1.2 Since 5 is a primitive root of 1 modulo 73, it has order 72, thus \(\zeta\)

4.1.4 Define \(L(s)\), show that it diverges for \(s = 1\) and converges absolutely for \(s > 1\).

4.1.5 Show that \(\prod_{\mathfrak{p} \text{ prime}} \frac{p}{p-1} \neq 1\) diverges.

4.1.6 Show that \(\prod_{\mathfrak{p} \text{ prime}} \frac{p}{p-1} = 0\). (Hint: note that \(\frac{p}{p-1} \cdot \frac{p}{p-1} = \frac{p^2}{p^2-1}\) and consider \(\zeta(2)\)).

4.1.7 Compute \(\sum_{m,n \geq 0} \frac{1}{\sqrt{mn}}\).

4.2.5 Let \(\epsilon(n) = 0, 1, -1\) if \(n \equiv 3, 0, 1, 2\). Define the Dirichlet L-series \(L = \sum_{n \geq 0} \frac{\epsilon(n)}{n^s}\)

4.3.4 Show that if \(M_l\) is a Mersenne prime, then \(l\) is prime.

4.3.5 Let \(\sigma(n)\) be the sum of all divisors of \(n\) (including 1 and \(n\)). If \(p\) is prime then compute \(\sigma(p^k)\). Show that if \(m, n\) are coprime, then \(\sigma(mn) = \sigma(m)\sigma(n)\).

5.1.1 \(5^2 = 25, 5^3 = 625, 5^4 = 762, 5^6 = 797, 5^{12} = -50, 5^{14} = 5128, 5^{16} = 318\cdot 762\cdot 625, 5^{20} = 25 \cdot 5 = 568 \cdot 944 = 1862\).

5.3.1 If \(x^a = 1\) and \(y^b = 1\), then \((xy)^n = x^ny^n = 1\cdot 1 = 1\) and \((x^{-1})^a = x^{-n} = (x^n)^{-1} = 1^{-1} = 1\). Moreover \(1^n = 1\). Therefore the set of all \(n\)-th roots is a non-empty subset of \(F^*\) closed under multiplication and inverses and hence it is a subgroup of \(F^*\).

5.3.2 Since \(\zeta\) is a primitive \(n\)-th root of 1, we have \(\zeta^n = 1\) and \(\zeta^k \neq 1\) for \(1 \leq k \leq n - 1\).

But then \(1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\) are distinct elements (if in fact \(\zeta^a = \zeta^b\) for \(0 \leq a < b \leq n - 1\), then \(\zeta^{b-a} = 1\) which is impossible as \(1 \leq b - a \leq n - 1\)). Clearly each \(\zeta^k\) is an \(n\)-th root of 1 (since \(\zeta^k)^n = \zeta^{nk} = (\zeta^n)^k = 1^k = 1\). We have that

\[
x^n - 1 = (x - 1)(x - \zeta)(x - \zeta^2) \cdots (x - \zeta^{n-1}) = x^n + \sum_{i=0}^{n-1} \zeta^i x^{n-i} + O(x)
\]
where \( \deg Q(x) = n - 2 \). Therefore equating the coefficients of \( x^{n-1} \) we get \( \sum_{i=0}^{n-1} \zeta^i = 0 \).

5.3.3 Since \( |(\mathbb{Z}/31\mathbb{Z})^*| = \varphi(31) = 30 \), the order of 3 divides 30 (by Lagrange’s theorem). Thus, if the order of 3 is not 30, then either 3^6 = 1 or 3^10 = 1 or 3^15 = 1. Now 3^5 = 243 = -5 so 3^10 = 25 = -6 so 3^15 = (-5)^3 = -125 = -1 and 3^6 = -15 are all \( \neq 1 \).

5.3.4 Find \( \zeta \) a primitive 12-th root of 1 in \( \mathbb{C}. \) What is the order of \( \zeta^2 \) and \( \zeta^3 \) in \( \mathbb{C}^* \)?

5.3.5 Given that \( 3 \) is a primitive root of 1 in \( F_{31} \), find all other primitive roots of 1 in \( F_{31} \). What is the order of 9?

5.3.6 Show that \( e^{it} = \cos(x) + i\sin(x) \) (formally) by comparing their taylor series expansions.

5.3.7 Show that

\[
(\cos(x) + i\sin(x))(\cos(y) + i\sin(y)) = \cos(x+y) + i\sin(x+y).
\]

(You can do this using the previous exercise or using the addition laws for sines and cosines.)

9.2.5 Given that (161,72) and (2889,1292) are the 2nd and 3rd solutions to \( X^2 - 5Y^2 = 1 \), find the 1st and 4th solution.

9.2.6 Given that (17,12) and (99,70) are the 2nd and 3rd solutions to \( X^2 - 2Y^2 = 1 \), find the 1st and 4th solution.

Math 4400, Fall 2014 solutions to the Extra homework.

3.2.3 \( (1+i)^{-1} = (1-i)(2-1)(1-i)6 = 6 + 5i \).

3.2.4 Since a field has no 0 divisors, it suffices to give 0 divisors.

\[
1^2 + 2^2 \equiv 5 \mod{5} \text{ so } (1+2i)(1-2i) = 0 \text{ in } F_5[i].
\]

\[
2^2 + 3^2 \equiv 13 \mod{13} \text{ so } (2+3i)(2-3i) = 0 \text{ in } F_{13}[i].
\]

3.2.5 In \( F_3[i] \) we have that the possible squares are \( 0^2 = 0 \), \( 1^2 = 1 \), \( 2^2 = 1 \) and so for \( a + ib \neq 0 \), \( N(a + ib) = a^2 + b^2 \in \{1, 2\} \) is always invertible and hence \( (a + ib)^{-1} = (a - ib)(a^2 + b^2)^{-1} \).

In \( F_7[i] \) we have that the possible squares are \( 0^2 = 0 \), \( 1^2 = 6^2 = 1 \), \( 2^2 = 5^2 = 4 \), \( 3^2 = 2^2 = 2 \) and so for \( a + ib \neq 0 \), \( N(a + ib) = a^2 + b^2 \in \{1, 2, 3, 4, 6\} \) is always invertible and hence \( (a + ib)^{-1} = (a - ib)(a^2 + b^2)^{-1} \).

3.2.6 If \( a, b \neq 0 \) and \( ab = 0 \), then \( a \) and \( b \) are 0 divisors. If \( a, b \in F \) a field and \( a \neq 0 \), then \( ab = 0 \) implies \( b = ab = a^{-1}ab = a^{-1}0 = 0 \).

3.2.7 Since \( F_{11}[i] \) is a field, \( F_{11}[i]^* \) is a group of order 120 so by Lagrange’s Theorem every element has order dividing 120 i.e. satisfies the equation \( x^{120} - 1 = 0 \). The only other element is 0 and hence every element satisfies the equation \( x^{121} - x = 0 \).

3.2.8 The non invertible elements of \( F_5[i] \) are the ones of norm 0. There are 9 such elements: 0, 1 + 2i, 1 - 2i, 2 + i, 2 - i, 1 + 3i, 1 - 3i, 3 + i, 3 - i, so \( |F_5[i]^*| = 16 \) so every element of \( F_5[i]^* \) satisfies \( x^{16} = 1 \). The elements 1 + 2i, 1 - 2i, 1 + 3i, 1 - 3i satisfy \( x^1 - x = 0 \), the elements 2 + i, 2 - i satisfy \( x^2 + x = 0 \) and the elements 3 + i, 3 - i satisfy \( x^2 - x = 0 \). Thus every element of \( F_5[i] \) satisfies the degree 24 polynomial \( x(x^{16} - 1)(x^3 - x)(x^2 - x)(x^2 + x) \).

3.2.9 We define \( f: F_3 \rightarrow F \) by \( f(0) = 0 \), \( f(1) = 1 \) and \( f(2) = 1 + 1 \). Since the characteristic of \( F \) is 3, 0, 1, 1 + 1 are distinct elements (but 1 + 1 + 1 = 0). Thus we see that we have identified \( F_3 \) with a subset of \( F \). We denote \( 1 + 1 \in F \) simply by 2. We must check that, this identification respects addition and multiplication. This can be done by checking all operations. Eg 2 + 2 = 1 in \( F_3 \) and \( (1 + 1) + (1 + 1) = 1 + (1 + 1) = 1 + 0 = 1 \) in \( F \) because \( 1 + 1 + 1 = 0 \).
as the characteristic of $F$ is $3$. Similarly, $2 \cdot 2 = 1$ in $F_3$ and $(1 + 1) \cdot (1 + 1) = (1 + 1) + (1 + 1) = 1 + (1 + 1 + 1) = 1 + 0 = 1$ in $F$.

3.2.10 By Lagrange’s Theorem, the elements of $F_3$ satisfy $x^3 - x = 0$ and the elements of $F_3[i]$ satisfy $i^4 - x = 0$ (since $F_3[i]$ is a field with 9 elements). Since the order of $F_3$ is 3, then its elements are the only ones to satisfy $x^3 - x = 0$. Therefore writing $x^3 - x = (x^3 - x)(x^6 + x^4 + x^2 + 1)$ it follows that the other 6 elements of $F_3[i]$ are precisely the solutions to $x^6 + x^4 + x^2 + 1 = 0$.

4.1.4 $L(s) = \sum_{i=1}^{\infty} \frac{1}{s+i}$. Now $\sum_{i=2}^{\infty} \frac{1}{i} \geq 2^k \cdot \frac{1}{2^k} \geq \frac{1}{2}$ because there are $2^k$ terms each $\geq \frac{1}{2^k}$.

The absolute convergence of $L(s)$ for $s > 1$ follows readily by the integral test from the convergence of $\int_1^\infty x^{-1} \, dx$.

4.1.5 For any $n > 0$, $n$ is the product of powers of prime numbers $p \leq n$ and so it is easy to see that $\sum_{i=1}^{n} \frac{1}{i} \leq \prod_{p \leq n \text{ prime}} \frac{p}{p-1}$ (recall that $\frac{p}{p-1} = 1 + \frac{1}{p} + \frac{1}{p^2} + \ldots$). But it is also easy to see that $\lim_{n \to \infty} \sum_{i=1}^{n} \frac{1}{i} = \infty$.

4.1.7 $\frac{1}{5}$, $\frac{3}{5}$.

5.3.4 $\zeta = e^{\pi i/6}$, $\zeta^2$ has order $12/2 = 6$ and $\zeta^3$ has order $12/3 = 4$.

5.3.5 $gcd(k, 30) = 1$ implies $k = 1, 7, 11, 13, 17, 19, 23, 29$ and so the primitive roots are $3, 3^1, 3^1, 3^{11}, 3^{13}, 3^{17}, 3^{19}, 3^{23}, 3^{29}$. The order of $9 = 2^3$ is $30/2 = 15$.

5.3.6 $e^{ix} = 1 + ix + \frac{(ix)^2}{2} + \frac{(ix)^3}{3} + \frac{(ix)^4}{4} + \frac{(ix)^5}{5} + \frac{(ix)^6}{6} + \ldots = 1 + ix - \frac{x^2}{2} - i \frac{x^3}{3} + \frac{x^4}{4} + \frac{x^5}{5} - \frac{x^6}{6} + \ldots$,

$(1 - \frac{x^2}{2} + \frac{x^4}{4} - \frac{x^6}{6} + \ldots) + i(x - \frac{x^3}{3} + \frac{x^5}{5} - \frac{x^7}{7} + \ldots) = \cos(x) + i\sin(x)$.

5.3.7 $(\cos(x) + i\sin(x))(\cos(y) + i\sin(y)) = (\cos(x)\cos(y) - \sin(x)\sin(y)) + i(\cos(x)\sin(y) + \sin(x)\cos(y)) = \cos(x + y) + i\sin(x + y)$.

Where we have used the addition laws for sines and cosines. Alternatively using (5.3.6) we have

$(\cos(x) + i\sin(x))(\cos(y) + i\sin(y)) = e^{ix} \cdot e^{iy} = e^{i(x+y)} = \cos(x + y) + i\sin(x + y)$.

9.2.5 The first solution is computed by

$$\frac{2889 + 1292\sqrt{5}}{161 + 72\sqrt{5}} = \frac{(2889 + 1292\sqrt{5})(161 - 72\sqrt{5})}{(161 + 72\sqrt{5})(161 - 72\sqrt{5})} = 9 + 4\sqrt{5}$$

and the forth solution is computed by

$$(161 + 72\sqrt{5})^2 = 51841 + 23184.$$