1.1.6 The continued fraction of 
\[1.1.5\quad 1 + \frac{\text{gcd}}{1.1.1}, \quad 3 + \frac{\text{gcd}}{1.2.1}, \quad 1 + \frac{\text{gcd}}{1.1.3} \]
\[1.1.7\quad 2\]
\[1.1.8\quad 1 + \frac{\text{gcd}}{1.2.2}, \quad \text{The solutions are } (1.2.4)\]
\[1.2.3\quad \text{Any solution must be divisible by the gcd, but}
\[1.2.5\quad \text{Since } a \text{ divides } c \text{, hence }
\[1.2.6\quad \text{If } g \text{ divides } a \text{, then } a = ga', b = gb'
\[1.2.7\quad \text{lcm} = 13853, 6951 = 13853 - 6951 / \text{gcd}(13853, 6951) = 13853 \cdot 6951 / 7 = 13756029, \]
\[1.3.2\quad \text{Since } p = a + b \text{ is prime, gcd}(a, p) = 1 \text{ so by the FTA, } 1 = ax + py = ax + (a + b)y = a(x + y) + by \text{ hence gcd}(a, b) = 1.\]
\[1.3.3\quad 3992003 = 1997 \cdot 1999 \text{ and } 1340939 = 1153 \cdot 1163.\]
\[1.4.1\quad \text{We have } 6 + 2\sqrt{3} = (1 - \sqrt{3})^2, \text{ and } 6 - 2\sqrt{3} = (1 - \sqrt{3})^2 \text{ so}
\[\frac{(1 + \sqrt{3})^{n+1} - (1 - \sqrt{3})^{n+1}}{2^{n+1}\sqrt{3}} + \frac{(1 + \sqrt{3})^n - (1 - \sqrt{3})^n}{2^n\sqrt{3}} =
\frac{(1 + \sqrt{3})^n(1 + \sqrt{3} + 2) - (1 - \sqrt{3})^n(1 - \sqrt{3} + 2)}{2^{n+2}\sqrt{3}} =\]
\[
\frac{(1 + \sqrt{3})^{n+2} - (1 - \sqrt{3})^{n+2}}{2^{n+2}\sqrt{3}}.
\]

Thus \(f_{n+2} = f_{n+1} + f_n\). To finish the proof we check that \(f_0 = f_1 = 1\) (easy check).

1.4.2 In the notation of the book \(b = r_a\). Assume for simplicity that \(n = 2m + 1\) is odd. Since \(b = r_n \geq 2r_{n-2} \geq 4r_{n-4} \geq 8r_{n-6} \geq 2^m r_1 \geq 2^m\), it follows that \(n = 2m + 1 = 2\log_2(2^m) + 1 \leq 2\log_2(b) + 1\). The case \(n\) is even is similar.

1.4.3 \(2\log_2(b) = 2\log_2(10)\log_10(b) > 6\log_10(b)\) and \(\log_10(b) + 1\) is \(\geq\) the number of digits of \(b\) (eg \(\log_10(10) + 1 = 2\)).

2.1.1 Suppose that \(e, e'\) are identities, then \(e = e \cdot e' = e'\) (the first equality follows as \(e'\) is an identity and the second as \(e\) is an identity).

2.1.2 Let \(b, b'\) be inverses of \(a\) so that \(ba = ab = ab' = b'a\), then \(b = b' = b(ab') = (ba)b' = e\).

2.1.3 We have \(e = (ab)^2 = abab\) thus \(a = aabab = ebab = bab\) and so \(ab = bba = bae = ba\).

2.1.4 Given \(kn, jn \in n\mathbb{Z}\), we have \(kn + jn = (k + j)n \in \mathbb{Z}\) so \(\mathbb{Z}\) is closed under addition.

Associativity: \((kn + jn) + ln = (k + j)n + ln = ((k + j) + l)n = (kn + jn) + ln\). Identity: \(0 = n0\), infact \(kn + 0n = (k + 0)n = kn = (0 + k)n = 0n + kn\). Inverses: the inverse of \(kn\) is \((-k)n\) since \(kn + (-k)n = (k - k)n = 0n = (0 + k)n = n\).

2.1.5 If \(H = \{0\}\), then \(H = 0\). If \(H \neq \{0\}\), then let \(n \in H\) be the smallest non-zero element in \(H\). Let \(h \in H\) be any other element and write \(h = nq + r\) where \(0 \leq r < n\). Since \(r = h - qn \in H\) and \(0 \leq r < n\), then by definition of \(n\) we have \(r = 0\) so that \(h \in n\mathbb{Z}\).

2.2.1 Since \(10 \equiv_{11} -1\), we have \(10^f \equiv_{11} (-1)^f\) and so \(m = \sum_{i=0}^{f} a_i 10^i \equiv_{11} \sum_{i=0}^{f} a_i (-1)^i\).

If \(11\) divides \(m\) then \(m \equiv_{11} 0\) so that \(0 \equiv_{11} \sum_{i=0}^{f} a_i (-1)^i\).

2.2.2 The sum of the digits is 33 which is not divisible by 9 and hence the number is not divisible by 9. The alternating sum of the digits is \(-11\) which is divisible by 11 and so the number is divisible by 11 (by the previous exercise).

2.2.3 \(\sum_{i=9}^{10} i \cdot y \equiv_{11} 2 \cdot 9 - 7\) so the number is \(3 - 540 = 78258 - 9\).

2.2.4 \(\sum_{i=0}^{10} i \cdot y \equiv_{11} 9 - 0\) so the number is \(0 - 31 = 030360 - 9\).

2.2.5 By assumption \(x - y = nk\) and \(y - z = nj\) so \(x - z = x - y + y - z = nk + nj = n(k + j)\) i.e. \(x \equiv_{n} z\).

2.3.6 1979 \(= 131 \cdot 15 + 14\), 131 \(= 14 \cdot 9 + 5\), 14 \(= 5 \cdot 2 + 4\), 5 \(= 4 + 1\), so the gcd is 1.

We have \(1 = 5 - 4 = 3 \cdot 5 - 14 = 3 \cdot 131 - 28 \cdot 14 = 423 \cdot 131 - 28 \cdot 1979\). Thus \(423 \cdot 131 \equiv_{1979} 1\) i.e. \(131^{-1} = 423\).

2.3.7 131 \(\equiv_{1979} 11\) so \(x = 131^{-1}11 = 423 \cdot 11 = 4653 = 695\) (modulo 1979).

2.3.8 1091 \(= 127 \cdot 8 + 75\), 127 \(= 75 + 52\), 75 \(= 52 + 23\), 52 \(= 23 + 6\), 23 \(= 6 \cdot 3 + 5\), 6 \(= 5 + 1\) so the gcd is 1.

We have \(1 = 6 - 5 = 6 \cdot 4 - 23 = 52 \cdot 4 - 23 \cdot 9 = 52 \cdot 13 - 75 \cdot 9 = 127 \cdot 13 - 75 \cdot 22 = 127 \cdot 189 - 1091 \cdot 22\). Thus \(127^{-1} = 189\) (modulo 1091).

2.3.9 127 \(\equiv_{1091} 11\) so \(x = 127^{-1} \cdot 11 = 189 \cdot 11 = 2079 = 988\) (modulo 1091).

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

2.4.2 \(\{Z/13Z\}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}\). \(<5> = \{5^0, 5^1, 5^2, 5^3\} = \{1, 5, 12, 8\}\) since \(5^4 = 1\) modulo 13. Note that \(<2> = \{2, 10, 11, 3\}\) and \(4 < 5 = \{4, 7, 9, 6\}\) We then have \(\{Z/13Z\}^* = <5> \cup <2> \cup <4\cdot 5>\) is the disjoint union of the three equivalence classes each of size 4 i.e. \(12 = 3 \cdot 4\).
2.5.5 We compute the last two digits of powers of two (i.e. $2^{2.5.4}$

2.5.2 1000

2.5.1 By the FTA we have $mx + ny = 1$ and by assumption $a = mk$ and $a = n j$. Therefore $k = knx + nky = nx + nky = n (x + ny)$, thus $a = mk = mn (x + ny)$ and $mn$ divides $a$.

2.5.5 1000 = 2353 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 $1 + 1 + 2 + 4 + 4 + 8 + 16 + 20 + 20 + 40 + 80 + 100 + 100 + 200 + 400 = 1000$.

2.5.3 $x \equiv 15$ implies $x = 5 + 11 k$ and so $5 + 11 k \equiv 13$ i.e. $11 k \equiv 13$ 2. The inverse of 11 modulo 13 is 6 (6·11 – 5·13 = 1) so $k \equiv 13$ 6·11 ·k \equiv 6·2 \equiv 13$ 2. Finally $x = 5 + 11 ·12 = 137$.

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

2.5.5 We compute the last two digits of powers of two (i.e. 2° modulo 100). 2° = 1, 2¹ = 2, 2² = 4, 2³ = 8, 2⁴ = 16, 2⁵ = 32, 2⁶ = 64, 2⁷ = 128, 2⁸ = 256, 2⁹ = 512, 2¹⁰ = 1024 = 16; 2¹¹ = 32, 2¹² = 64, 2¹³ = 128, 2¹⁴ = 256, 2¹⁵ = 512, 2¹⁶ = 1024 = 16; 2¹⁷ = 32, 2¹⁸ = 64, 2¹⁹ = 128, 2²⁰ = 256, 2²¹ = 512, 2²² = 1024 = 16; 2²³ = 32, 2²⁴ = 64, 2²⁵ = 128, 2²⁶ = 256, 2²⁷ = 512, 2²⁸ = 1024 = 16; 2²⁹ = 32, 2³⁰ = 64, 2³¹ = 128, 2³² = 256, 2³³ = 512, 2³⁴ = 1024 = 16; 2³⁵ = 32, 2³⁶ = 64, 2³⁷ = 128, 2³⁸ = 256, 2³⁹ = 512, 2⁴⁰ = 1024 = 16.

4.1 Hint: $\int (x/2)^2 dx = x^3/12$. $\int (x/2)^2 dx = \sum (-1)^k (x/2)^{2k} dx$ integrating by parts $\int (x/2)^{2k} dx = x^{2k}/(2k) = x^{2k}/k$. Then $\int -\cos (kx) dx = \sum (-1)^k \cos (kx) dx$ and $\int -\cos (kx) dx = 0$ and $\int -\cos (kx) dx = (k^2 + 1)^{1/2}$.

4.2.1 Define $\varphi (n) = 0, 1, 0, -1$ if $n \equiv 4, 1, 2, 3$ and let

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

= $\prod_{p \equiv 4 \text{ or } 1} (1 + \frac{1}{p} + \frac{1}{p^2} + \ldots) \prod_{p \equiv 3 \text{ or } 0} (1 - \frac{1}{p} + \frac{1}{p^2} + \ldots)$. If there are finitely many $p \equiv 4$, then this behaves like

$$\prod_{p \equiv 4 \text{ or } 1} (1 + \frac{1}{p} + \frac{1}{p^2} + \ldots) \prod_{p \equiv 3 \text{ or } 0} (1 - \frac{1}{p} + \frac{1}{p^2} + \ldots) \prod_{p \equiv 1 \text{ or } 1} \frac{p}{p+1} = 0.$$ If there are finitely many $p \equiv 4$, then this behaves like

$$\prod_{p \equiv 4 \text{ or } 1} (1 + \frac{1}{p} + \frac{1}{p^2} + \ldots) \prod_{p \equiv 3 \text{ or } 0} (1 - \frac{1}{p} + \frac{1}{p^2} + \ldots) \prod_{p \equiv 1 \text{ or } 1} \frac{p}{p+1} = +\infty.$$ The above argument is not correct because $L$ is not absolutely convergent. However, let $L(s) = \sum_{n \geq 1} (\frac{\varphi (n)}{n}) s$, then $L(s)$ is absolutely convergent for all $s > 1$ and taking the limit as $s \to 1$, the above argument becomes correct.

4.2.2 We know that $\prod_{p \equiv 1 \text{ or } 1} \frac{p}{p+1} = +\infty$ and $\prod_{p \equiv 3 \text{ or } 0} \frac{p}{p+1} = 0$. But then $\prod_{p \equiv 1 \text{ or } 1} \frac{p}{p+1} = +\infty$ (prove this using $\lim_{n \to \infty} \prod_{p \equiv 1 \text{ or } 1} \frac{p}{p+1} = +\infty$). It is easy to check that $\frac{p}{p+1} \geq \frac{p}{2}$, so $\prod_{p \equiv 1 \text{ or } 1} \frac{p}{p+1} = +\infty$. Thus $\prod_{p \equiv 2 \text{ or } 2} \frac{p}{p+1} \geq \prod_{p \equiv 2 \text{ or } 2} \frac{p}{p+1} = +\infty$. $\sigma (3^k - 1) = (3^{k+1} - 1)/(3 - 1)$. Now $3^2 \equiv 1$ so $3^{k+2} = (3^2)^{k+1} \equiv 1$ 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.

4.3.2 The number of digits is $\log(2^{32} \cdot 582.657 - 1)$. The number is about $\frac{32 \cdot 582.657}{1000} \log(2)$.

5.1.1 Modulo 1979, we have $5^2 = 25$, $5^4 = 625$, $5^8 = 390625 = 762$, $5^{16} = 762^2 = 580644 = 797$, $5^{32} = 797^2 = 635209 = 1929 = -50$, $5^{64} = 25$, $5^{128} = 625$ and so $5^{143} = 5^{128} \cdot 5^4 = 5^5 \cdot 625 \cdot 762 \cdot 625 \cdot 25 \cdot 5 = 99625 = 675$.

5.1.3 The order of $(\mathbb{Z}/\mathbb{Z}_{15})^*$ is $\varphi(35) = \varphi(5) \varphi(7) = 4 \cdot 6 = 24$. Since 24 and 11 are coprime, write $1 = 11 \cdot 1 - 5 \cdot 24$ and we can solve $x^{11} =_{35} 13$ by letting $x = 13^{11}$. We have $13^2 = 169 = -6$, $13^3 = 36 = 1$ and so $x = 13^{11} = 13^3 = -6 \cdot 13 = -78 = -8$. (Note that $(-8)^2 = 64 = -6$ and $(-8)^3 = (-6)^2 = 1$ and so $(-8)^{11} = (-8)^3 = -8 \cdot -6 = 48 = 13$.)

5.3.1 Let $\mu_n$ be the set of all $n$-th roots of 1 in $F^*$. 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

$$x^n - 1 = (x - 1)(x - \zeta) \cdots (x - \zeta^{n-1})$$

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 $3^2 = 9$, $3^3 = 27$, $3^6 = 9 \cdot 27 = 9 \cdot (-4) = -36 = -5$, $3^5 = -15$, $3^{10} = 25$ and $3^5 = -125 = -1$ are all $\neq 1$.

The 6-th roots of 1 are $3^0 = 1$, $3^5 = -5$, $3^{10} = 25$, $3^{15} = -1$, $3^{20} = 5$ 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 $x = 27 = 7$.

5.4.2 $I(4) + I(2) = I(9)$ so $2 + 2I(x) = 6$ (modulo 10) so $I(x) = 2$, $7$ so $x = 2^2 = 4$ or $x = 2^7 = 7$.

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 $I(x) = -7 \cdot 5 \cdot I(x) = -7 \cdot 6 = -42 \equiv_{18} 12$ 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 $6^{(p-1)/2} = 6^{30} = 18 \cdot 25 = 450 = 40 = -1$. (But we knew this as $6^{30}$ is a square root of 1 so is $\pm 1$, but it can’t be 1 as otherwise the order of 6 would be $\leq 20$ but we assumed it is a primitive root i.e. it has order 40.)

6.2.2 $2^{(31-1)/2} = 2^{15} = 32^3 = 13 = 1$ so 2 is a square mod 31. 315 = $(27)^5 = (-4)^5 = -1 \cdot 2^5 = 32 = -1$ (as $2^5 = 32 = 1$ mod 31). So 3 is not a square modulo 31.

6.3.1 The order of 6 is 40, so the order of $g = 6^5$ is 8. Now, $g = 6^5 = 36 \cdot 36 \cdot 6 = (-5)^2 \cdot 6 = 150 = 27$. We also have $g^7 = g^{-1} = 3$ (as $1 = 2 \cdot 41 - 3 \cdot 27$). So $g + g^7 = 24$ is a square root of 2.

6.3.2 The order of 5 is 72 (in $\mathbb{F}_{73}$). So $g = 5^9$ has order 8. Now $g = 5^9 = (125)^3 = (-21)^3 = -441 \cdot 21 = 3 \cdot 21 = 63$. 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 $g = 3 + 4 \cdot 3 = 15 = -2$ 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 \( \left( \frac{-2}{11} \right) = \left( \frac{2}{11} \right) \left( \frac{-1}{11} \right) \).

Since \( 131 \equiv 3 \mod 4 \), we have \( \left( \frac{3}{11} \right) = -1 \) and since \( 131 \equiv 3 \mod 3 \), we have \( \left( \frac{3}{11} \right) = -1 \).

Thus \( \left( \frac{-2}{11} \right) = (-1)^2 = 1 \) and we can solve this equation.

8.1.1 \( 221 = 13 \cdot 17 = (3^2 + 2^2)(4^2 + 3^2) = 142^2 + 5^2 \).

8.1.2 \( 8^2 + 1^2 = 5 \cdot 13 \). Pick \( 5/2 < u = -2, v = 1 \leq 5/2 \) 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 \((5^{18})^2 = 5^{36} \equiv_{73} 1\). 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 \( 5 < u = -3, v = 1 \leq 5 \) and so \( xu + yv = -80, xv - yu = 30 \) and dividing by 10 we have \( 8^2 + 3^2 = 64 + 9 = 73 \).

8.1.4 Suppose \( p \equiv 1 \pm 1 \), then \( 2 = b^2 \) and so a necessary condition is to solve \( x^2 + z^2 \equiv_p 0 \) where \( z = by \). If \( p \equiv -1 \), then \( p \equiv 4 \) and so there is no such solution. If \( p \equiv 1 \), then \( p \equiv 4 \) and so there is a solution, i.e. we can write \( x^2 + z^2 = kp \) for some \( 0 < x, z < p \) and \( k > 0 \). Letting \( y = b^{-1}z \), we may assume that \( x^2 + 2y^2 = kp \). By an argument similar to Fermat descent, we hope to show that \( x^2 + 2y^2 = p \) has a solution.

Suppose \( p \equiv 3 \pm 1 \), then \((x/y)^2 \equiv_p -2\). If \( p \equiv 8 \), then \( p \equiv 4 \) and so \( -1 = b^2 \) (modulo \( p \)). But then \((x/y)^2 \equiv_p 2 \) which is impossible as 2 is not a square. If \( p \equiv 8 \), then \( p \equiv 4 \) and so both 2 and \(-1\) are not squares and hence \(-2\) is a square, say \( -2 = b^2 \) (modulo \( p \)). But then \((x/y)^2 \equiv_p 1\) has a solution, e.g. \( x = by \) so that \( x^2 + b^2 \equiv_p 0 \) i.e. \( x^2 + 2y^2 = kp \). By an argument similar to Fermat descent, we hope to show that \( x^2 + 2y^2 = p \) has a solution.

8.1.5 Complete this computation, but the formula is wrong. It should be:

\[
(x^2 + 2y^2)(u^2 + 2v^2) = (xu - 2yv)^2 + 2(yu + xv)^2.
\]

8.1.6 \( 8^2 + 2 = 6 \cdot 11 \) = \((2^2 + 2 \cdot 1^2)(3^2 + 2 \cdot 1^2) \) = \((2 \cdot 3 - 2 \cdot 1 \cdot 1) + 2(1 \cdot 3 - 2 \cdot 1) = 4^2 + 2 \cdot 3^2 \).

8.2.1 \((11 + 7i) = 2(5 + 3i) + (1 + i) \) and \((5 + 3i) = (4 - i)(1 + i) \) so \( gcd((11 + 7i), (5 + 3i)) = 1 + i \).

8.2.2 \( N(11 + 3i) = 130 \) so the primes have norm 2, 5 or 13. The irreducible elements with \( N(x) = 2 \) are \( 1 + i \). Then we see \((11 + 3i) = (1 + i)(7 - 4i) \). The irreducible elements with \( N(x) = 5 \) are \( 2 \pm i \) and one sees that \((7 - 4i) = (2 + i)(2 - 3i) \). Since \( N(2 - 3i) = 13, (2 - 3i) \) is irreducible.

**Math 4400, Fall 2014 Extra Homework.**

3.2.3 Find the inverse of \( 1 + i \) in \( F_{11}[i] \).

3.2.4 Show that \( F_3[i] \) and \( F_7[i] \) are not fields. (Hint: solve \( a^2 + b^2 = 0 \) and give a zero divisor.)

3.2.5 Show that \( F_3[i] \), \( F_7[i] \) and \( F_{11}[i] \) are fields. (Hint: compute all possible values of \( a^2 + b^2 \).

3.2.6 What is a zero divisor and why do fields not have any zero divisors?

3.2.7 Show that every element of \( F_{11}[i] \) satisfies the equation \( x^{121} - x = 0 \).

3.2.8 Repeat 3.2.7 for \( F_5[i] \). (Hint: compute \( F_5[i]^* \).

3.2.9 Explain why \( F_3 \) is contained in any field \( F \) of characteristic 3.

3.2.10 Explain why the solutions to \( x^6 + x^4 + x^2 + 1 \) are exactly the elements of \( F_3[i] \) \( \setminus \ F_3 \).

3.2.11 If \( a + bi \in F_p[i] \) then let \( N(a + bi) = a^2 + b^2 \). Show that \( N((a + bi)(c + id)) = N(a + bi)N(c + id) \) and deduce that \( a + bi \in F_p[i] \) if and only if \( N(a + bi) \neq 0 \).
4.1.4 Define $L(s)$, show that it diverges for $s = 1$ and converges absolutely for $s > 1$.
4.1.5 Show that $\prod_{p \text{ prime}} \frac{p}{p-1}$ diverges.
4.1.6 Show that $\prod_{p \text{ prime}} \frac{p}{p+1} = 0$. (Hint: note that $\frac{p}{p-1} \frac{p}{p+1} = \frac{p^2}{p^2-1}$ and consider $\zeta(2)$).
4.1.7 Compute $\sum_{n \geq 0} \frac{1}{2^n}$.
4.2.5 Let $\epsilon(n) = 0$, $1$ if $n \equiv 3 \mod 1, 2$. Define the Dirichlet L-series $L = \sum_{n \geq 0} \frac{\epsilon(n)}{n}$.
Show that this series converges to a value $\frac{1}{2} < L < 1$ and show that

$$L = \prod_{p \text{ prime}} \left( \sum_{j \geq 0} \frac{\epsilon(p^j)}{p^j} \right).$$

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 $\sigma(p^n)$. Show that if $m, n$ are coprime, then $\sigma(mn) = \sigma(m)\sigma(n)$.
5.1.1 $5^2 = 25$, $5^3 = 125$, $5^6 = 732$, $5^{10} = 250$, $5^{12} = 5^2 = 521$, $5^{128} = 318$, $5^{143} = 51285^4 5^{225} = 318762 - 255 = 568094 = 1862$.
5.3.1 If $x^a = 1$ and $y^a = 1$, then $(xy)^a = x^ay^a = 1 \cdot 1 = 1$ and $(x^{-1})^a = x^{-a} = (x^a)^{-1} = 1^{-1} = 1$. Moreover $1^a = 1$. 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 $\zeta^a = 1$ and $\zeta^k \neq 1$ for $1 \leq k < n - 1$. 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 $\zeta^{kn} = \zeta^n k = 1^{k} = 1$). We have that

$$x^n - 1 = (x - 1)(x - \zeta)(x - \zeta^2) \cdots (x - \zeta^{n-1}) = x^n + (\sum_{i=0}^{n-1} \zeta^i)x^{n-1} + O(x)$$

where $\deg O(x) = n - 2$. 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 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 $\mathbb{F}_{31}$, find all other primitive roots of 1 in $\mathbb{F}_{31}$. What is the order of 9?
5.3.6 Show that $e^{ix} = \cos(x) + isin(x)$ (formally) by comparing their taylor series expansions.
5.3.7 Show that

$$(\cos(x) + isin(x))(\cos(y) + isin(y)) = \cos(x + y) + isin(x + y).$$

(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.

\[1^2 + 2^2 \equiv_5 0 \text{ so } (1 + 2i)(1 - 2i) = 0 \in F_5[i].\]

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

3.2.5 In \(F_5[i]\) 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 \(0^2 = 0, 1^2 = 6^2 = 1, 2^2 = 5^2 = 4, 3^2 = 4^2 = 2\) 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 \(F_3[i]\) 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 \(|F_3[i]^+| = 16\) so every element of \(F_3[i]^+\) satisfies \(x^{16} = 1\). The elements 1 + 2i, 1 - 2i, 1 + 3i, 1 - 3i satisfy \(x^3 - x = 0\), 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 \(F_3[i]\) satisfies the degree 24 polynomial \(x(x^6 - 1)(x^3 - x)(x^2 - x)(x + x^2)\).

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 = 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 \((1 + 1) + (1 + 1) = 1 + (1 + 1 + 1) = 1 + 0 = 1\) in \(F\) because 1 + 1 + 1 = 0 as the characteristic of \(F\) is 3. Similarly, 2·2 = 1 in \(F_3\) and (1 + 1)·(1 + 1) = (1 + 1) + (1 + 1 + 1) = 1 + 0 = 1 in \(F\).

3.2.10 By Lagrange’s Theorem, the elements of \(F_3[i]\) satisfy \(x^3 - x = 0\) and the elements of \(F_3[i]\) satisfy \(x^9 - x = 0\) (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 \(x^9 - x = (x^3 - x)(x^6 + x^4 + x^2 + 1)\) 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 \(L(x) = \sum_{i=1}^{\infty} \frac{1}{p^i}\). Now \(\sum_{i=2}^{k+1} \frac{1}{i} \geq 2^k \cdot \frac{1}{2^{k+1}} \geq \frac{1}{2}\) because there are \(2^k\) terms each \(\geq \frac{1}{2^k}\). Then \(\sum_{k=0}^{\infty} \frac{1}{i} \geq 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{1} + \frac{1}{8} + \frac{1}{16} + \frac{1}{32} = \lim_{k \to \infty} \sum_{i=1}^{k} \frac{1}{i} = \lim_{k \to \infty} (1 + \frac{k+1}{2}) = \infty.

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

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 \(\sum_{i=1}^{\frac{n}{p} \leq n} \frac{1}{p} \leq \frac{1}{p^2} \prod_{p \leq n} p\). (recall that \(\frac{1}{p^2} = 1 + \frac{1}{p} + \frac{1}{p^2} + \ldots\)). But it is also easy to see that \(\lim_{n \to \infty} \sum_{i=1}^{\frac{n}{p}} \frac{1}{2} = \infty\).

4.1.7 \(\frac{1}{6} = \frac{1}{6}\).

5.3.4 \(\zeta = e^{i\pi/6}\) has order 12/2 = 6 and \(\zeta^2\) 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 \(3, 3^7, 3^{11}, 3^{13}, 3^{17}, 3^{19}, 3^{23}, 3^{29}\). The order of \(g = 3^2\) is 30/2 = 15.
\[ e^{ix} = 1 + ix + \frac{(ix)^2}{2} + \frac{(ix)^3}{3} + \frac{(ix)^4}{4} + \frac{(ix)^5}{5} + \frac{(ix)^6}{6} + \ldots = \]
\[ = 1 + ix - \frac{x^2}{2} - i\frac{x^3}{3} + \frac{x^4}{4} + i\frac{x^5}{5} - \frac{x^6}{6} + \ldots = \]
\[ (1 - \frac{x^2}{2} + \frac{x^4}{4} - \frac{x^6}{6} + \ldots) + i(x - \frac{x^3}{3} + \frac{x^5}{5} - \frac{x^7}{7} + \ldots) = \]
\[ = \cos(x) + i\sin(x). \]

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

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