Exercises from *A Classical Introduction to Modern Number Theory* by Kenneth Ireland and Michael Rosen

Exercise 1.27 For all odd n show that $8 \mid n^2 - 1$.

Exercise 1.30 Prove that $\frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$ is not an integer.

Exercise 1.31 Show that 2 is divisible by $(1+i)^2$ in $\mathbb{Z}[i]$.

Exercise 2.4 If a is a nonzero integer, then for $n > m$ show that $\left(a^{2^n} + 1, a^{2^m} + 1\right) =$ 1 or 2 depending on whether a is odd or even.

Exercise 2.21 Define $\wedge(n) = \log p$ if n is a power of p and zero otherwise. Prove that $\sum_{A|n} \mu(n/d) \log d = \wedge(n)$.

Exercise 2.27a Show that $\sum' 1/n$, the sum being over square free integers, diverges.

Exercise 3.1 Show that there are infinitely many primes congruent to -1 modulo 6 .

Exercise 3.4 Show that the equation $3x^2 + 2 = y^2$ has no solution in integers.

Exercise 3.5 Show that the equation $7x^3 + 2 = y^3$ has no solution in integers.

Exercise 3.10 If n is not a prime, show that $(n-1)! \equiv 0(n)$, except when $n = 4$.

Exercise 3.14 Let p and q be distinct odd primes such that $p - 1$ divides $q - 1$. If $(n, pq) = 1$, show that $n^{q-1} \equiv 1(pq)$.

Exercise 3.18 Let N be the number of solutions to $f(x) \equiv 0(n)$ and N_i be the number of solutions to $f(x) \equiv 0\,(p_i^{a_i})$. Prove that $N = N_1 N_2 \cdots N_i$.

Exercise 3.20 Show that $x^2 \equiv 1\left(2^b\right)$ has one solution if $b = 1$, two solutions if $b = 2$, and four solutions if $b \geq 3$.

Exercise 4.4 Consider a prime p of the form $4t+1$. Show that a is a primitive root modulo p iff $-a$ is a primitive root modulo p.

Exercise 4.5 Consider a prime p of the form $4t+3$. Show that a is a primitive root modulo p iff $-a$ has order $(p-1)/2$.

Exercise 4.6 If $p = 2^n + 1$ is a Fermat prime, show that 3 is a primitive root modulo p.

Exercise 4.8 Let p be an odd prime. Show that a is a primitive root modulo p iff $a^{(p-1)/q} \not\equiv 1(p)$ for all prime divisors q of $p-1$.

Exercise 4.9 Show that the product of all the primitive roots modulo p is congruent to $(-1)^{\phi(p-1)}$ modulo p.

Exercise 4.10 Show that the sum of all the primitive roots modulo p is congruent to $\mu(p-1)$ modulo p.

Exercise 4.11 Prove that $1^k + 2^k + \cdots + (p-1)^k \equiv 0(p)$ if $p-1 \nmid k$ and $-1(p)$ if $p-1 \mid k$.

Exercise 4.22 If a has order 3 modulo p, show that $1+a$ has order 6 .

Exercise 4.24 Show that $ax^m + by^n \equiv c(p)$ has the same number of solutions as $ax^{m'} + by^{n'} \equiv c(p)$, where $m' = (m, p-1)$ and $n' = (n, p-1)$.

Exercise 5.2 Show that the number of solutions to $x^2 \equiv a(p)$ is given by $1 + (a/p)$.

Exercise 5.3 Suppose that $p \nmid a$. Show that the number of solutions to $ax^2 + bx + c \equiv 0(p)$ is given by $1 + \left(\left(b^2 - 4ac\right)/p\right)$.

Exercise 5.4 Prove that $\sum_{a=1}^{p-1}(a/p) = 0$.

Exercise 5.5 Prove that $\sum_{\substack{p-1\\x=0}}((ax+b)/p) = 0$ provided that $p \nmid a$.

Exercise 5.6 Show that the number of solutions to $x^2 - y^2 \equiv a(p)$ is given by $\sum_{y=0}^{p-1} \left(1 + \left(\left(y^2 + a\right)/p\right)\right)$.

Exercise 5.7 By calculating directly show that the number of solutions to $x^2 - y^2 \equiv a(p)$ is $p-1$ if $p \nmid a$ and $2p-1$ if $p \mid a$.

Exercise 5.13 Show that any prime divisor of $x^4 - x^2 + 1$ is congruent to 1 modulo 12 .

Exercise 5.27 Suppose that f is such that $b \equiv af(p)$. Show that $f^2 \equiv -1(p)$ and that $2^{(p-1)/4} \equiv f^{ab/2}(p)$

Exercise 5.28 Show that $x^4 \equiv 2(p)$ has a solution for $p \equiv 1(4)$ iff p is of the form $A^2 + 64B^2$.

Exercise 5.37 Show that if a is negative then $p \equiv q(4a) together with p \not| a$ imply $(a/p) = (a/q)$.

Exercise 6.18 Show that there exist algebraic numbers of arbitrarily high degree.

Exercise 7.6 Let $K \supset F$ be finite fields with $[K : F] = 3$. Show that if $\alpha \in F$ is not a square in F, it is not a square in K.

Exercise 7.24 Suppose that $f(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ has the property that $f(x+y) = f(x) +\ f(y) \in \mathbb{Z}/p\mathbb{Z}[x, y]$. Show that $f(x)$ must be of the form $a_0x + a_1x^p + a_2x^{p^2} + \cdots + a_mx^{p^m}$.

Exercise 12.12 Show that $\sin(\pi/12)$ is an algebraic number.

Exercise 12.22 Let $F \subset E$ be algebraic number fields. Show that any isomorphism of F into $\mathbb{C}$ extends in exactly $[E : F]$ ways to an isomorphism of E into $\mathbb{C}$.

Exercise 12.30 Let p be an odd prime and consider $\mathbb{Q}(\sqrt{p})$. If $q \neq p$ is prime show that $\sigma_q(\sqrt{p}) = (p/q)\sqrt{p}$ where σ_q is the Frobenius automorphism at a prime ideal in $\mathbb{Q}(\sqrt{p})$ lying above q.

Exercise 18.1 Show that $165x^2 - 21y^2 = 19$ has no integral solution.

Exercise 18.4 Show that 1729 is the smallest positive integer expressible as the sum of two different integral cubes in two ways.

Exercise 18.32 Let d be a square-free integer $d \equiv 1$ or 2 modulo 4 . Show that if x and y are integers such that $y^2 = x^3 - d$ then $(x, 2d) = 1$.