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

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

Proof. We have $n^2 - 1 = (n+1)(n-1)$. Since n is odd, both $n+1, n-1$ are even, and moreso, one of these must be divisible by 4 , as one of the two consecutive odd numbers is divisible by 4 . Thus, their product is divisible by 8 . Similarly, if 3 does not divide n, it must divide one of $n-1, n+1$, otherwise it wouldn't divide three consecutive integers, which is impossible. As n is odd, $n+1$ is even, so $(n+1)(n-1)$ is divisible by both 2 and 3 , so it is divisible by 6 . $\square$

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

Proof. Let 2^s be the largest power of 2 occuring as a denominator in H_n, say $2^s = k \leqslant n$. Write $H_n = \frac{1}{2^s} + (1 + 1/2 + \ldots + 1/(k-1) + 1/(k+1) + \ldots + 1/n$. The sum in parentheses can be written as $1/2^{s-1}$ times sum of fractions with odd denominators, so the denominator of the sum in parentheses will not be divisible by 2^s, but it must equal 2^s by Ex 1.29. $\square$

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

Proof. We have $(1+i)^2 = 1 + 2i - 1 = 2i$, so $2 = -i(1+i)^2$. $\square$

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.

Proof.

$$\operatorname{ord}_p n! = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor \leq \sum_{k \geq 1} \frac{n}{p^k} = \frac{n}{p} \frac{1}{1 - \frac{1}{p}} = \frac{n}{p-1}$$

The decomposition of $n!$ in prime factors is
$n! = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ where $\alpha_i = \operatorname{ord}_{p_i} n! \leq \frac{n}{p_i - 1}$, and $p_i \leq n,\ i = 1, 2, \cdots, k$.

Then

$$
\begin{aligned}
n! &\leq p_1^{\frac{n}{p_1-1}} p_2^{\frac{n}{p_2-1}} \cdots p_k^{\frac{n}{p_n-1}} \\
\sqrt[n]{n!} &\leq p_1^{\frac{1}{p_1-1}} p_2^{\frac{1}{p_2-1}} \cdots p_k^{\frac{1}{p_n-1}} \\
&\leq \prod_{p\leq n} p^{\frac{1}{p-1}}
\end{aligned}
$$

(the values of p in this product describe all prime numbers $p \leq n$.) $\square$

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

Proof.

$$
\begin{cases}
\wedge(n) = \log p & \text{if } n = p^\alpha,\ \alpha \in \mathbb{N}^* \\
 = 0 & \text{otherwise.}
\end{cases}
$$

Let $n = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ the decomposition of n in prime factors. As $\wedge(d) = 0$ for all divisors of n, except for $d = p_j^i, i > 0, j = 1, \ldots t$,

$$
\begin{aligned}
\sum_{d|n} \wedge(d) &= \sum_{i=1}^{\alpha_1} \wedge(p_1^i) + \cdots + \sum_{i=1}^{\alpha_t} \wedge(p_t^i) \\
&= \alpha_1 \log p_1 + \cdots + \alpha_t \log p_t \\
&= \log n
\end{aligned}
$$

By Mobius Inversion Theorem,

$$
\wedge(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \log d.
$$

$\square$

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

Proof. Let $S \subset \mathbb{N}^*$ the set of square free integers.

Let $N \in \mathbb{N}^*$. Every integer n, $1 \leq n \leq N$ can be written as $n = ab^2$, where a, b are integers and a is square free. Then $1 \leq a \leq N$, and $1 \leq b \leq \sqrt{N}$, so

$$
\sum_{n\leq N} \frac{1}{n} \leq \sum_{a\in S, a\leq N} \ \sum_{1\leq b\leq\sqrt{N}} \frac{1}{ab^2} \leq \sum_{a\in S, a\leq N} \frac{1}{a} \sum_{b=1}^{\infty} \frac{1}{b^2} = \frac{\pi^2}{6} \sum_{a\in S, a\leq N} \frac{1}{a}.
$$

So

$$
\sum_{a\in S, a\leq N} \frac{1}{a} \geq \frac{6}{\pi^2} \sum_{n\leq N} \frac{1}{n}.
$$

As $\sum_{n=1}^{\infty} \frac{1}{n}$ diverges, $\lim\limits_{N\to\infty} \sum\limits_{a\in S, a\leq N} \frac{1}{a} = +\infty$, so the family $\left(\frac{1}{a}\right)_{a\in S}$ of the inverse of square free integers is not summable.

Let $S_N = \prod_{p<N}(1+1/p)$, and $p_1, p_2, \ldots, p_l$ $(l = l(N))$ all prime integers less than N. Then

$$\begin{aligned} S_N &= \left(1+\frac{1}{p_1}\right)\cdots\left(1+\frac{1}{p_l}\right) \\ &= \sum_{(\varepsilon_1,\cdots,\varepsilon_l)\in\{0,1\}^l} \frac{1}{p_1^{\varepsilon_1}\cdots p_l^{\varepsilon_l}} \end{aligned}$$

We prove this last formula by induction. This is true for $l = 1 :$ $\sum_{\varepsilon\in\{0,1\}} 1/p_1^{\varepsilon} = 1 + 1/p_1$.

If it is true for the integer l, then

$$\begin{aligned} \left(1+\frac{1}{p_1}\right)\cdots\left(1+\frac{1}{p_l}\right)\left(1+\frac{1}{p_{l+1}}\right) &= \sum_{(\varepsilon_1,\ldots,\varepsilon_l)\in\{0,1\}^l} \frac{1}{p_1^{\varepsilon_1}\cdots p_l^{\varepsilon_l}}\left(1+\frac{1}{p_{l+1}}\right) \\ &= \sum_{(\varepsilon_1,\ldots,\varepsilon_l)\in\{0,1\}^l} \frac{1}{p_1^{\varepsilon_1}\cdots p_l^{\varepsilon_l}} + \sum_{(\varepsilon_1,\ldots,\varepsilon_l)\in\{0,1\}^l} \frac{1}{p_1^{\varepsilon_1}\cdots p_l^{\varepsilon_l} p_{l+1}} \\ &= \sum_{(\varepsilon_1,\ldots,\varepsilon_l,\varepsilon_{l+1})\in\{0,1\}^{l+1}} \frac{1}{p_1^{\varepsilon_1}\cdots p_l^{\varepsilon_l} p_{l+1}^{\varepsilon_{l+1}}} \end{aligned}$$

So it is true for all l.

Thus $S_N = \sum_{n\in\Delta} \frac{1}{n}$, where Δ is the set of square free integers whose prime factors are less than N.

As $\sum 1/n$, the sum being over square free integers, diverges, $\lim\limits_{N\to\infty} S_N = +\infty$:

$$\lim_{N\to\infty} \prod_{p<N} \left(1+\frac{1}{p}\right) = +\infty.$$

$e^x \geq 1 + x, x \geq \log(1+x)$ for $x > 0$, so

$$\log S_N = \sum_{k=1}^{l(N)} \log\left(1+\frac{1}{p_k}\right) \leq \sum_{k=1}^{l(N)} \frac{1}{p_k}.$$

$\lim\limits_{N\to\infty} \log S_N = +\infty$ and $\lim\limits_{N\to\infty} l(N) = +\infty$, so

$$\lim_{N\to\infty} \sum_{p<N} \frac{1}{p} = +\infty.$$

$\square$

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

Proof. Let n any integer such that $n \geq 3$, and $N = n! - 1 = 2 \times 3 \times \cdots \times n - 1 > 1$.

Then $N \equiv -1 \pmod 6$. As $6k+2, 6k+3, 6k+4$ are composite for all integers k, every prime factor of N is congruent to 1 or -1 modulo 6. If every prime factor of N was congruent to 1, then $N \equiv 1 \pmod 6$: this is a contradiction because $-1 \not\equiv 1 \pmod 6$. So there exists a prime factor p of N such that $p \equiv -1 \pmod 6$.

If $p \leq n$, then $p \mid n!$, and $p \mid N = n! - 1$, so $p \mid 1$. As p is prime, this is a contradiction, so $p > n$.

Conclusion :

for any integer n, there exists a prime $p > n$ such that $p \equiv -1 \pmod 6$: there are infinitely many primes congruent to -1 modulo 6. $\square$

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

Proof. If $3x^2 + 2 = y^2$, then $\overline{y}^2 = \overline{2}$ in $\mathbb{Z}/3\mathbb{Z}$.

As $\{-1, 0, 1\}$ is a complete set of residues modulo 3, the squares in $\mathbb{Z}/3\mathbb{Z}$ are $\overline{0} = \overline{0}^2$ and $\overline{1} = \overline{1}^2 = (\overline{-1})^2$, so $\overline{2}$ is not a square in $\mathbb{Z}/3\mathbb{Z}$: $\overline{y}^2 = \overline{2}$ is impossible in $\mathbb{Z}/3\mathbb{Z}$.

Thus $3x^2 + 2 = y^2$ has no solution in integers. $\square$

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

Proof. If $7x^2 + 2 = y^3$, $x, y \in \mathbb{Z}$, then $y^3 \equiv 2 \pmod 7$ (so $y \not\equiv 0 \pmod 7$)

From Fermat's Little Theorem, $y^6 \equiv 1 \pmod 7$, so $2^2 \equiv y^6 \equiv 1 \pmod 7$, which implies $7 \mid 2^2 - 1 = 3$: this is a contradiction. Thus the equation $7x^2 + 2 = y^3$ has no solution in integers. $\square$

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

Proof. Suppose that $n > 1$ is not a prime. Then $n = uv$, where $2 \leq u \leq v \leq n - 1$.

• If $u \neq v$, then $n = uv \mid (n-1)! = 1 \times 2 \times \cdots \times u \times \cdots \times v \times \cdots \times (n-1)$ (even if $u \wedge v \neq 1$!).

• If $u = v$, $n = u^2$ is a square.

If u is not prime, $u = st$, $2 \leq s \leq t \leq u - 1 \leq n - 1$, and $n = u'v'$, where $u' = s, v' = st^2$ verify $2 \leq u' < v' \leq n - 1$. As in the first case, $n = u'v' \mid (n-1)!$.

If $u = p$ is a prime, then $n = p^2$.

In the case $p = 2$, $n = 4$ and $n = 4 \nmid (n-1)! = 6$. In the other case $p > 2$, and $(n-1)! = (p^2-1)!$ contains the factors $p < 2p < p^2$, so $p^2 \mid (p^2-1)!, n \mid (n-1)!$.

Conclusion : if n is not a prime, $(n-1)! \equiv 0 \pmod n$, except when $n = 4$. $\square$

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

Proof. As $n \wedge pq = 1, n \wedge p = 1, n \wedge q = 1$, so from Fermat's Little Theorem

$$n^{q-1} \equiv 1 \pmod q, \qquad n^{p-1} \equiv 1 \pmod p.$$

$p-1 \mid q-1$, so there exists $k \in \mathbb{Z}$ such that $q-1 = k(p-1)$. Thus

$$n^{q-1} = (n^{p-1})^k \equiv 1 \pmod p.$$

$p \mid n^{q-1}-1, q \mid n^{q-1}-1$, and $p \wedge q = 1$, so $pq \mid n^{q-1}-1$:

$$n^{q-1} \equiv 1 \pmod{pq}.$$

□

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 $N = N_1 N_2 \cdots N_i$.

Proof. Note $[x]_n$ the class of x modulo n. Let S the set of solutions in $\mathbb{Z}/n\mathbb{Z}$ of $f(\overline{x}) = 0$, and S_i the set of solutions in $\mathbb{Z}/p^{a_i}\mathbb{Z}$ of $f(\overline{x}) = 0$.

(We designate with the same letter the polynomial f in $\mathbb{Z}[x]$ or its reduction in $\mathbb{Z}/n\mathbb{Z}[x]$.)

Let

$$\varphi : \left\{ \begin{array}{ccc} S & \to & S_1 \times S_2 \times \cdots \times S_t \\ [x]_n & \mapsto & ([x]_{p_1^{a_1}}, [x]_{p_2^{a_2}}, \ldots, [x]_{p_t^{a_t}}) \end{array} \right.$$

• φ is well defined : if $x \equiv x' \pmod n$, then $x \equiv x' \pmod{p_i^{a_i}}$, $i = 1, 2, \cdots, t$, so $([x]_{p_1^{a_1}}, [x]_{p_2^{a_2}}, \ldots, [x]_{p_t^{a_t}}) = ([x']_{p_1^{a_1}}, [x']_{p_2^{a_2}}, \ldots, [x']_{p_t^{a_t}})$. Moreover, we proved in Ex 3.17 that $[x]_n \in S \Rightarrow [x]_{p_i^{a_i}} \in S_i$.

• φ is injective : if $([x]_{p_1^{a_1}}, [x]_{p_2^{a_2}}, \ldots, [x]_{p_t^{a_t}}) = ([x']_{p_1^{a_1}}, [x']_{p_2^{a_2}}, \ldots, [x']_{p_t^{a_t}})$, then $p_i^{a_i} \mid x'-x$, $i = 1, 2, \ldots, t$, so $n \mid x'-x$ and $[x]_n = [x']_n$.

• φ is surjective : if $y = ([x_1]_{p_1^{a_1}}, [x_2]_{p_2^{a_2}}, \ldots, [x_t]_{p_t^{a_t}})$ is any element of $S_1 \times S_2 \times \cdots \times S_t$, there exists from Chinese remainder theorem $x \in \mathbb{Z}$ such that $x \equiv x_i \pmod{p_i^{a_i}}$. Then $\varphi([x]_n) = y$ (see Ex. 3.17).

In conclusion, a φ is bijective, $N = |S| = |S_1 \times S_2 \times \cdots \times S_t| = N_1 N_2 \cdots N_t$.

□

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.

Proof. Suppose that a is a primitive root modulo p. As $p-1$ is even, $(-a)^{p-1} = a^{p-1} \equiv 1$ (mod$p$) If $(-a)^n \equiv 1($mod$p)$, with $n \in \mathbb{N}$, then $a^n \equiv (-1)^n($mod$p)$. Therefore $a^{2n} \equiv 1($mod$p)$. As a is a primitive root modulo $p, p-1 | 2n, 2t | n$, so n is even.

Hence $a^n \equiv 1(\bmod p)$, and $p-1 \mid n$. So the least $n \in \mathbb{N}^*$ such that $(-a)^n \equiv 1$ $(\bmod p)$ is $p-1$: the order of $-a$ modulo p is $p-1, -a$ is a primitive root modulo p. Conversely, if $-a$ is a primitive root modulo p, we apply the previous result at $-a$ to to obtain that $-(-a) = a$ is a primitive root. □

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 $(p-1)/2$.

Proof. Let a a primitive root modulo p. As $a^{p-1} \equiv 1(\bmod p), p \mid \left(a^{(p-1)/2}-1\right)\left(a^{(p-1)/2}+1\right)$, so $p \mid a^{(p-1)/2}-1$ or $p \mid a^{(p-1)/2}+1$. As a is a primitive root modulo $p, a^{(p-1)/2} \not\equiv 1(\mathrm{mod} p)$, so

$$a^{(p-1)/2} \equiv -1 \pmod{p}.$$

Hence $(-a)^{(p-1)/2} = (-1)^{2t+1}a^{(p-1)/2} \equiv (-1) \times (-1) = 1(\mathrm{mod} p)$. Suppose that $(-a)^n \equiv 1(\mathrm{mod} p)$, with $n \in \mathbb{N}$. Then $a^{2n} = (-a)^{2n} \equiv 1(\mathrm{mod} p)$, so $p-1 \,\big|\, 2n, \frac{p-1}{2} \,\big|\, n$. So $-a$ has order $(p-1)/2$ modulo p. Conversely, suppose that $-a$ has order $(p-1)/2 = 2t+1$ modulo p. Let $2, p_1, \ldots p_k$ the prime factors of $p-1$, where p_i are odd. $a^{(p-1)/2} = a^{2t+1} = -(-a)^{2t+1} = -(-a)^{(p-1)/2} \equiv -1$, so $a^{(p-1)/2} \not\equiv 1(\mathrm{mod} 2)$. As $p-1$ is even, $(p-1)/p_i$ is even, so $a^{(p-1)/p_i} = (-a)^{(p-1)/p_i} \not\equiv 1(\mathrm{mod} p)$(since $-a$ has order $p-1$). So the order of a is $p-1$ (see Ex. 4.8) : a is a primitive root modulo p. $\square$

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

Proof. Write $p = 2^k+1$, with $k = 2^n$.

We suppose that $n > 0$, so $k \geq 2, p \geq 5$. As p is prime, $3^{p-1} \equiv 1 \pmod{p}$.

In other words, $3^{2^k} \equiv 1 \pmod{p}$: the order of 3 is a divisor of 2^k, a power of 2.

3 has order 2^k modulo p iff $3^{2^{k-1}} \not\equiv 1 \pmod{p}$. As $\left(3^{2^{k-1}}\right)^2 \equiv 1 \pmod{p}$, where p is prime, this is equivalent to $3^{2^{k-1}} \equiv -1 \pmod{p}$, which remains to prove.

$3^{2^{k-1}} = 3^{(p-1)/2} \equiv \left(\frac{3}{p}\right) \pmod{p}$.

As the result is true for $p = 5$, we can suppose $n \geq 2$. From the law of quadratic reciprocity :

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{(p-1)/2} = (-1)^{2^{k-1}} = 1.$$

So $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$

$$\begin{aligned} p = 2^{2^n}+1 &\equiv (-1)^{2^n}+1 \pmod{3} \\ &\equiv 2 \equiv -1 \pmod{3}, \end{aligned}$$

so $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = -1$, that is to say

$$3^{2^{k-1}} \equiv -1 \pmod{p}.$$

The order of 3 modulo $p = 2^{2^n}+1$ is $p-1 = 2^{2^n}$: 3 is a primitive root modulo p.

(On the other hand, if 3 is of order $p-1$ modulo p, then p is prime, so

$$F_n = 2^{2^n} + 1 \text{ is prime} \iff 3^{(F_n-1)/2} = 3^{2^{2^n-1}} \equiv -1 \pmod{F_n}.)$$

$\square$

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 $p-1$.

Proof. • If a is a primitive root, then $a^k \not\equiv 1$ for all $k, 1 \leq k < p-1$, so $a^{(p-1)/q} \not\equiv 1 \pmod p$ for all prime divisors q of $p-1$.

• In the other direction, suppose $a^{(p-1)/q} \not\equiv 1 \pmod p$ for all prime divisors q of $p-1$.

Let δ the order of a, and $p-1 = q_1^{a_1} q_2^{a_2} \cdots q_k^{a_k}$ the decomposition of $p-1$ in prime factors. As $\delta \mid p-1, \delta = q_1^{b_1} p_2^{b_2} \cdots q_k^{b_k}$, with $b_i \leq a_i, i = 1, 2, \ldots, k$. If $b_i < a_i$ for some index i, then $\delta \mid (p-1)/q_i$, so $a^{(p-1)/q_i} \equiv 1 \pmod p$, which is in contradiction with the hypothesis. Thus $b_i = a_i$ for all i, and $\delta = q-1 :$ a is a primitive root modulo p. $\square$

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 $p-1 \mid k$.

Proof. Let $S_k = 1^k + 2^k + \cdots + (p-1)^k$.

Let g a primitive root modulo p : $\overline{g}$ a generator of $\mathbb{F}_p^*$.

As $(\overline{1}, \overline{g}, \overline{g}^2, \ldots, \overline{g}^{p-2})$ is a permutation of $(\overline{1}, \overline{2}, \ldots, \overline{p-1})$,

$$\begin{aligned}
\overline{S_k} &= \overline{1}^k + \overline{2}^k + \cdots + \overline{p-1}^k \\
&= \sum_{i=0}^{p-2} \overline{g}^{ki} = \begin{cases} \overline{p-1} = -\overline{1} & \text{if} \quad p-1 \mid k \\ \frac{\overline{g}^{(p-1)k} - 1}{\overline{g}^k - 1} = \overline{0} & \text{if} \quad p-1 \nmid k \end{cases}
\end{aligned}$$

since $p-1 \mid k \iff \overline{g}^k = \overline{1}$.

Conclusion :

$$\begin{aligned}
1^k + 2^k + \cdots + (p-1)^k &\equiv 0 \pmod p \text{ if } p-1 \nmid k \\
1^k + 2^k + \cdots + (p-1)^k &\equiv -1 \pmod p \text{ if } p-1 \mid k
\end{aligned}$$

$\square$

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

Proof. • As $a^6 + 1 = (a^2+1)(a^4 - a^2 + 1)$, $p \mid a^4 - a^2 + 1$ implies $p \mid a^6 + 1$, so $\left(\frac{-1}{p}\right) = 1$ and $p \equiv 1 \pmod 4$.

• $p \mid 4a^4 - 4a^2 + 4 = (2a-1)^2 + 3$, so $\left(\frac{-3}{p}\right) = 1$.

As $-3 \equiv 1 \pmod 4$, $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$, so $\left(\frac{p}{3}\right) = 1$, thus $p \equiv 1 \pmod 3$.
$4 \mid p-1$ and $3 \mid p-1$, thus $12 \mid p-1$:

$$p \equiv 1 \pmod{12}.$$

□

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

Proof. If $p \equiv 1$ [4] and if there exists $x \in \mathbb{Z}$ such that $x^4 \equiv 2$ [p], then

$$2^{\frac{p-1}{4}} \equiv x^{p-1} \equiv 1 \ [p].$$

From Ex. 5.27, where $p = a^2 + b^2, a$ odd, we know that

$$f^{\frac{ab}{2}} \equiv 2^{\frac{p-1}{4}} \equiv 1 \ [p].$$

Since $f^2 \equiv -1$ [p], the order of f modulo p is 4, thus $4 \mid \frac{ab}{2}$, so $8 \mid ab$.
As a is odd, $8|b$, then $p = A^2 + 64B^2$ (with $A = a, B = b/8$).

Conversely, if $p = A^2 + 64B^2$, then $p \equiv A^2 \equiv 1$ [4].
Let $a = A, b = 8B$. Then

$$2^{\frac{p-1}{4}} \equiv f^{\frac{ab}{2}} \equiv f^{4AB} \equiv (-1)^{2AB} \equiv 1 \ [p].$$

As $2^{\frac{p-1}{4}} \equiv 1$ [p], $x^4 \equiv 2$ [p] has a solution in $\mathbb{Z}$ (Prop. 4.2.1) : 2 is a biquadratic residue modulo p.
Conclusion :

$$\exists A \in \mathbb{Z}, \exists B \in \mathbb{Z}, p = A^2 + 64B^2 \iff (p \equiv 1 \ [4] \text{ and } \exists x \in \mathbb{Z},\ x^4 \equiv 2 \ [p]).$$

□

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

Proof. Write $a = -A, A > 0$. As $p \equiv q \pmod{4a}$, we know from Prop. 5.3.3. (b) that $(A/p) = (A/q)$.
Moreover,

$$\left(\frac{a}{p}\right) = \left(\frac{-A}{p}\right) = (-1)^{(p-1)/2}\left(\frac{A}{p}\right)$$
$$\left(\frac{a}{q}\right) = \left(\frac{-A}{q}\right) = (-1^{(q-1)/2}\left(\frac{A}{q}\right)$$

As $p \equiv q \pmod{4a}$, $p = q + 4ak, k \in \mathbb{Z}$, so

$$(-1)^{(p-1)/2} = (-1)^{(q+4ak-1)/2} = (-1)^{(q-1)/2},$$

so $(a/p) = (a/q)$. □

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

Proof.

$$\begin{aligned}\sin \pi/12 = \sin(\pi/4 - \pi/6) &= \sin \pi/4 \cos \pi/6 - \cos \pi/4 \sin \pi/6 \\ &= \frac{\sqrt{3}}{2\sqrt{2}} - \frac{1}{2\sqrt{2}} \\ &= \frac{\sqrt{3}-1}{2\sqrt{2}}\end{aligned}$$

□

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.

Proof. Let $n = a^3 + b^3$, and suppose that $\gcd(a, b) = 1$. If a prime $p \mid a^3 + b^3$, then

$$\left(ab^{-1}\right)^3 \equiv_p -1$$

Thus $3 \mid \frac{p-1}{2}$, that is, $p \equiv_6 1$. If we have $n = a^3 + b^3 = c^3 + d^3$, then we can factor n as

$$\begin{aligned} n &= (a+b)\left(a^2 - ab + b^2\right) \\ n &= (c+d)\left(c^2 - cd + d^2\right)\end{aligned}$$

Thus we need n to have atleast 3 disctinct prime factors, and so the smallest taxicab number is on the form

$$n = (6k+1)(12k+1)(18k+1)$$

□