1. Prove that $12 + 5\sqrt{7}$ is a prime in the ring of algebraic integers $\mathcal{O} \subset \mathbb{Q}((\sqrt{7})$. (We recall that a prime $\alpha \in \mathcal{O}$ is an element that is divisible only by elements invertible in $\mathcal{O}$, and by elements that are products of $\alpha$ by some invertible element) (Use properties of the norm).

2. Solve $x^{39} \equiv 3 \mod 13$.

3. Find all integers $n$ such that $\phi(n) = n/6$. (Remember that $\phi(n)$ is the number of integers $k$ such that $1 \leq k \leq n$ and $(k,n) = 1$).

4. Suppose that $a$ has a square root in $\mathbb{Z}_p$, for $p$ prime, and suppose further that $p \equiv 5 \mod 8$.

Show that one of the values $x = a^{p+3}/8$ or $x = (2a)(4a)^{(p-5)/8}$ is a solution to the congruence $x^2 \equiv a \mod p$.

5. We call $\sigma(n)$ the sum of all positive divisors of integer $n$.

For example $\sigma(6) = 1 + 2 + 3 + 6 = 12$, and $\sigma(5) = 1 + 5 = 6$.

1. For any prime $p$, any integer $k > 1$, show that $\sigma(p^k) = \frac{p^{k+1} - 1}{p-1}$.

2. If $(m,n) = 1$ prove that $\sigma(mn) = \sigma(m)\sigma(n)$. You will probably want to start with a simpler case $\sigma(pq) = \sigma(p)\sigma(q)$, when $p,q$ are two distinct primes.

3. Give a general formula for $\sigma(n)$ in terms of its decomposition in prime factors $n = p_1^{k_1} \ldots p_n^{k_n}$.

6. 1. Show that there is no invertible element $\alpha \in \mathbb{Z}[\sqrt{2}]$ such that $1 < \alpha < 1 + \sqrt{2}$.

2. Deduce that any invertible element (greater than 0) of $\mathbb{Z}[\sqrt{2}]$ is a power of $1 + \sqrt{2}$.

7. Let $\alpha = 1 + \sqrt{2}$. Write $\alpha^n = u_n + v_n\sqrt{2}$. Show that $u_n^2 - 2v_n^2 = 1$. 


8. Expand $\sqrt{20}$ into a continued fraction. Justify your answer.

9. Use inequalities that can be found in the proof of theorem 7.7 on the page 332 to find a rational number $p/q$ such that $|\sqrt{5} - p/q| < 1/q^2$, $q \geq 5$.

10. Show that if $p$ is prime and $a$ is an integer not divisible by $p$, then there exist integers $x$ and $y$ such that $ax \equiv y \mod p$, with $0 < |x| < \sqrt{p}$ and $0 < |y| < \sqrt{p}$. (Hint: consider all the integers of the form $au - v$ with $0 \leq u \leq \lfloor \sqrt{p} \rfloor$, $0 \leq v \leq \lfloor \sqrt{p} \rfloor$ where $\lfloor \cdot \rfloor$ denotes the integer part, and show that there must be two of them that are congruent modulo $p$, then form the difference of these two integers).

11. Show that if a prime number $p \neq 2$ can be written as a sum $a^2 + b^2$ then necessarily one has $p \equiv 1 \mod 4$.

12. Explain why $-1$ has a square root in $\mathbb{Z}_p$, when $p$ is a prime of the form $4n + 1$.

13. Use results of problems 10-12 to show that if $p$ prime is congruent to 1 modulo 4, then $p$ can be written as the sum of two squares. (In the process of the proof you will construct a pair of integers $x, y$ such that $0 < x^2 + y^2 < 2p$ and $p | x^2 + y^2$).

14. Suppose that you have two groups of recipients. Both of them use the same number $n$, but use two different exponents $e_1, e_2$ such that $(e_1, e_2) = 1$. Assume that the same message $P$ is sent to the two groups. Therefore you have two public encrypted messages $C_1 \equiv P^{e_1} \mod n$ and $C_2 \equiv P^{e_2} \mod n$.

Show that knowing these two encrypted messages one can recover the initial message $P$.

15. Let $p$ be an odd prime and let $d = b^2 - 4ac$. Show that the congruence $ax^2 + bx + c \equiv 0 \mod p$ is equivalent to the congruence $y^2 \equiv d \mod p$, where $y = 2ax + b$. Conclude that if $d \equiv 0 \mod p$, then there is exactly one solution modulo $p$; if $d$ has a square root in $\mathbb{Z}_p$, then there are two
(non congruent) solutions; and if $d$ has no square root in $\mathbb{Z}_p$, then there are no solutions. What about the case $p = 2$?

16. The curve $y^2 = x^3 + 8$ contains the points $(1, 3)$ and $(7/4, 13/8)$. The line through these two points intersects the curve in exactly one other point. Find it and explain why its coordinates are rational numbers.