7.3.2. Let
\[ n = N(\rho) \]
\[ = \rho \bar{\rho}. \]
Then \( n \) is an integer and \( \rho \) divides \( n \). As \( \rho \) is a prime it is not a unit and so \( n > 1 \). Let \( n = p_1 p_2 \ldots p_k \) be the prime factorisation of \( n \). As \( \rho \) is a prime, \( \rho \) must divide one of the factors of the prime factorisation of \( n \), so that \( \rho \) must divide a prime \( p = p_i \).

7.3.3. If \( 1+i \) divides \( a+bi \) then \( 2 = N(1+i) \) divides \( N(a+bi) = a^2 + b^2 \). Thus \( a \equiv b \mod 2 \).

Now suppose \( a \equiv b \mod 2 \). If \( a \) and \( b \) are even then \( 2 \) divides \( a + bi \) so that \( 1+i \) divides \( a + bi \). Suppose that \( a \) and \( b \) are both odd. Then
\[ a + bi - (1 + i) = (a - 1) + (b - 1)i. \]
As \( a - 1 \) and \( b - 1 \) are both even, \( (a - 1) + (b - 1)i \) is divisible by \( 1 + i \), so that \( a + bi \) divides \( 1 + i \).

7.3.4. If \( n \) is square-free and
\[ x^2 + y^2 = n \]
then \( (x, y) = 1 \). Thus every representation of a sum of squares is automatically a primitive representation. It follows that \( p_2(n) = r_2(n) \).

If \( n \) is square-free then \( 4 \) does not divide \( n \). Theorem 7.5 implies that \( p_2(n) = 0 \) if and only if there is a prime \( p \equiv 3 \mod 4 \) dividing \( n \) and Theorem 7.6 implies that \( r_2(n) = 0 \) under the same conditions. If there is no prime congruent to \( 3 \) modulo \( 4 \) dividing \( n \) then
\[ \tau(n') = 2^s, \]
so that Theorem 7.3 and Theorem 7.5 imply \( p_2(n) = r_2(n) \).

7.3.6. Define a function
\[ f : \mathbb{N} \rightarrow \mathbb{Z} \]
by the rule
\[ f(m) = \begin{cases} 
0 & \text{if } m \text{ is even} \\
1 & \text{if } m \equiv 1 \mod 4 \\
-1 & \text{if } m \equiv 3 \mod 4.
\end{cases} \]
We check that
\[ f(ab) = f(a)f(b) \]
case by case. If $a$ or $b$ is even then so is $ab$ and both sides are zero. If $a$ and $b$ are both congruent to 1 modulo 4 then so is $ab$ and both sides are equal to 1. If $a \equiv 1 \mod 4$ and $b \equiv 3 \mod 4$ then $ab \equiv 3 \mod 4$ and both sides are $-1$. By symmetry we just need to consider the case when both $a$ and $b \equiv 3 \mod 4$. In this case $ab \equiv 1 \mod 4$ and both sides are equal to 1.

It follows that

$$F(n) = \sum_{d|n} f(d)$$

is multiplicative.

Note that

$$F(n) = \sum_{d|n} f(d)$$

$$= \sum_{d|n, d\equiv 1 \mod 4} f(d) + \sum_{d|n, d\equiv 3 \mod 4} f(d)$$

$$= \sum_{d|n, d\equiv 1 \mod 4} 1 - \sum_{d|n, d\equiv 3 \mod 4} 1$$

$$= \tau_1(n) - \tau_3(n).$$

By (4.6) we just have to show that

$$\delta \tau(n_1) = F(n) \quad \text{where} \quad n = 2^u n_1 n_2,$$

$n_1$ is a product over primes congruent to 1 modulo 4, $n_2$ is a product over primes congruent to 3 modulo 4, and

$$\delta = \begin{cases} 
1 & \text{if } n_2 \text{ is a square} \\
0 & \text{otherwise}. 
\end{cases}$$

Since both sides of this equation are multiplicative, it suffices to check what happens when $n = p^e$ is a power of a prime.

There are three cases. If $p = 2$ then $n_1 = 1$, $\delta = 1$ and

$$F(n) = F(2^e)$$

$$= 1$$

$$= \delta \tau(n_1).$$

If $p \equiv 1 \mod 4$ then $n_1 = n$, $\delta = 1$ and

$$F(n) = F(p^e)$$

$$= (1 + e)$$

$$= \delta \tau(n_1).$$

2
If \( p \equiv e \mod 4 \) then \( n_1 = 1, \delta = 1 \) unless \( e \) is odd and
\[
F(p^e) = \begin{cases} 
1 & \text{if } e \text{ is even} \\
0 & \text{if } e \text{ is odd.}
\end{cases}
\]

7.3.7. Consider the Diophantine equation
\[ x^2 + 1 = y^n, \]
where \( n > 1 \). We look for solutions with \( x > 0 \).
If \( x \) is odd then the LHS is even. It follows that the RHS is divisible by 4, as \( n > 1 \). But then \( x^2 \) is congruent to 3 modulo 4, a contradiction.

Now suppose that \( n = 2m \) is even. Then
\[ y^n - 1 = (y^m - 1)(y^m + 1). \]
The only possible common factor of \( y^m - 1 \) and \( y^m + 1 \) is 2. As \( x^2 \) is a square, it follows that \( n \) is not even.
Note that
\[ x^2 + 1 = (x + i)(x - i). \]
If \( \rho \) divides both \( x + i \) and \( x - i \) then \( \rho \) must divide \( 2i \), so that \( \rho \) divides 2. As \( x \) is an odd integer it follows that \( \rho \) is a unit. Thus \( (x + i, x - i) = 1 \).
If \( \rho \) is a Gaussian prime that divides \( x + i \) then \( \rho \) must divide \( y \) but it cannot divide \( x - i \). Suppose that the largest power of \( \rho \) which divides \( y \) is \( \rho^e \). As \( \rho^en \) divides \( y^n \) it follows that \( \rho^en \) divides \( x + i \), but no larger power. It follows that \( x + i = (a + bi)^n \) is an \( n \)th power.
As \( x + i = (a + bi)^n \), if we split this equation into its real and imaginary parts, we get
\[
x = a^n - \binom{n}{2} a^{n-2}b^2 + \binom{n}{4} a^{n-4}b^4 + \ldots \quad \text{and} \quad 1 = \binom{n}{1} a^{n-1}b - \binom{n}{3} a^{n-3}b^3 + \ldots.
\]
Note that \( b \) divides every term of the RHS of the second expansion. As the LHS is 1, it follows that \( b = \pm 1 \).
In this case the equations reduce to
\[ 1 = a^n - \binom{n}{2} a^{n-2} + \binom{n}{4} a^{n-4} + \ldots \quad \text{and} \quad \pm 1 = a^{n-1} - \binom{n}{3} a^{n-3} + \ldots. \]
If \( n = 3 \) the second equation reduces to
\[ \pm 1 = 3a^2 - 1. \]
Thus either \( a = 0 \) or \( 3a^2 = 2 \), not possible.
If \( n = 5 \) the second equation reduces to
\[ \pm 1 = 5a^4 - 10a^2 + 1. \]
Thus either
\[ a^2 = 5 \quad \text{or} \quad 5a^4 - 10a^2 + 2 = 0. \]
Neither of these equations have integral solutions.
If \( n = 7 \) the second equation reduces to
\[ \pm 1 = 7a^6 - 35a^4 + 21a^2 - 1. \]
Thus either
\[ a^4 - 5a^2 + 3 = 0 \quad \text{or} \quad 7a^6 - 35a^4 + 21a^2 - 2 = 0. \]
If we view the first equation as a quadratic in \( a^2 \), then there are no rational roots, so no rational roots for \( a \) either. The second equation has no integer roots.

7.4.1. An integer is not representable as the sum of three cubes if and only if it is of the form \( 4^k(8k + 7) \). The number of integers up to \( N \) which are divisible by \( 4^k \) is
\[ \frac{N}{4^k}. \]
The number of such integers congruent to 7 modulo 8 is at least
\[ \frac{\lfloor \frac{N}{8} \rfloor}{4^k}. \]
Note that these numbers don’t overlap, since if \( N = 4^km \) and \( m \) is congruent to 7 modulo 8, then \( N \) is not divisible by \( 4^{k+1} \). The number of integers up to \( N \) which are not representable as the sum of three cubes is then the sum
\[ \sum \frac{\lfloor \frac{N}{8} \rfloor}{4^k}. \]
If we remove the round down we get
\[ \sum \frac{N}{8 \cdot 4^k}, \]
a geometric series. If we sum the geometric series we get
\[ \frac{N}{8(1 - 3/4)} = \frac{N}{6}. \]
The error is at most twice the number of terms in the sum, which is at most
\[ 2 \log_4 N. \]
If we divide this by \( N \) then the ratio goes to zero.

7.4.2. If \( p = 2 \) then take \( x = y = 1 \) and \( z = 0 \). Otherwise let \( z = 1. \)
We have to solve
\[ x^2 + y^2 + c \equiv 0 \mod p. \]
Note that there are \((p + 1)/2\) distinct non-zero numbers of the form 

\[ ax^2 \quad \text{and} \quad -bz^2 + c, \]

modulo \(p\), since 

\[ ai^2 \equiv aj^2 \mod p \quad \text{implies that} \quad i^2 \equiv j^2 \mod p, \]

and we already saw in lectures that the latter are distinct if \(0 \leq i < j \leq (p - 1)/2\).

Since 

\[ \frac{p + 1}{2} + \frac{p + 1}{2} = p + 1 > p, \]

unless \(p = 3\), it follows that we can choose \(ax^2\) and \(-by^2 + c\) so that they coincide for some choice of \(x\) and \(y\). Thus we can solve the original equation.

7.4.3. We show that every integer is of the form 

\[ \pm x^2 \pm y^2 \pm z^2. \]

We may assume that \(n\) is a natural number. As 

\[ 2n + 1 = (n + 1)^2 - n^2, \]

it follows that every odd natural number is the difference of two squares. If \(n\) is even then \(n + 1\) is odd. If \(n + 1 = x^2 - y^2\) then 

\[ n = x^2 - y^2 - 1^2. \]

Suppose that 

\[ 6 = \pm x^2 \pm y^2. \]

At least one term is positive. Possibly switching \(x\) and \(y\) we have 

\[ 6 = x^2 \pm y^2. \]

Consider the equation 

\[ x^2 + y^2 = 6. \]

\(x\) and \(y\) are both at most two and it is easy to see there is no solution. Otherwise we have 

\[ x^2 - y^2 = 6. \]

As 

\[ x^2 - y^2 = (x - y)(x + y), \]

either \(x - y = 1\) and \(x + y = 6\) or \(x - y = 2\) and \(x + y = 3\). In both cases, neither \(x\) nor \(y\) are natural numbers.

Thus \(6\) requires all three terms.
7.4.4. We check to see that $-2$ is a residue of $p$. We have

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{2}{p}\right).$$

If $p \equiv 1 \mod 8$ then $p \equiv 1 \mod 4$ and so $-1$ is a residue of $p$. On the other hand, $2$ is also a quadratic residue of $p$, so that $-2$ is a residue of $p$.

If $p \equiv 3 \mod 8$ then $p \equiv 3 \mod 4$ and so $-1$ is not a residue of $p$. On the other hand, $2$ is also not a quadratic residue of $p$, so that $-2$ is a residue of $p$.

Thus $-2$ is a residue of $p$ if $p \equiv 1$ or $3 \mod 8$. By (7.2.2) it follows that we may find $x$ and $y$ such that

$$x^2 + 2y^2 = p.$$ 

But then

$$x^2 + y^2 + y^2 = p.$$