MODEL ANSWERS TO THE FIRST HOMEWORK

7.1.1. By assumption r is a quadratic residue of p. Let s be the inverse of r modulo p. It follows that s is also a quadratic residue of p. Pick a such that $a^2 \equiv s \mod p$. Apply (1.2) to a and $\lambda = g$. Then we may find u and v such that

$$au \equiv v \mod p$$

where $0 < u < g$ and $0 < |v| \leq p/g$. As v is an integer it follows that $0 < |v| \leq h$. Squaring both sides gives

$$su^2 \equiv v^2 \mod p.$$

Multiplying both sides by r gives

$$s^2 \equiv rv^2 \mod p.$$

7.1.2. Suppose that we consider integers $x_1, x_2, \dots, x_s$ such that $|x_j| \leq H$. If

$$y_i = \sum_j a_{ij}x_j$$

then

$$\begin{aligned} |y_i| &= \left|\sum_j a_{ij}x_j\right| \\ &\leq \sum_j |a_{ij}x_j| \\ &= \sum_j |a_{ij}||x_j| \\ &\leq \sum_j AH \\ &= sAH. \end{aligned}$$

The number of choices of s-stuples $(x_1, x_2, \dots, x_s)$ is then $(2H+1)^s$ and the number of possible r-tuples $(y_1, y_2, \dots, y_r)$ is as most $(2sAH+1)^r$. If

$$(2sAH + 1)^r < (2H + 1)^s,$$

then by the pigeonhole principle we must have two different s-tuples $(x_1, x_2, \dots, x_s)$ and $(w_1, w_2, \dots, w_s)$ which give rise to the same r-tuple $(y_1, y_2, \dots, y_r)$.

The difference $(u_1 = x_1 - w_1, u_2 = x_2 - w_2, \dots, u_r = x_r - w_r)$ is then a solution to the system of linear homogeneous equations.
If

$$2H + 1 \geq (sA)^{r/(s-r)}$$

then

$$\begin{aligned}(2sAH + 1)^r &< (sA(2H + 1))^r \\ &= (sA)^r (2H + 1)^r \\ &= (sA)^r (2H + 1)^{r-s} (2H + 1)^s \\ &< (2H + 1)^s.\end{aligned}$$

7.2.2. (a) Pick u such that $u^2 \equiv -1 \mod p$. By (1.2) we may find r and s such that

$$us \equiv r \mod p$$

where $0 < s < \sqrt{p}$ and $|r| \leq \sqrt{p}$. If $r > 0$ then put $x = s$ and $y = r$. If $r < 0$ then put $x = -r$ and $y = s$. As $u(-r) \equiv s \mod p$, either way we have $ux \equiv y \mod p$, $0 < x < \sqrt{p}$ and $0 < y < \sqrt{p}$.
Note that $x^2 + y^2 \equiv 0 \mod p$. As

$$\begin{aligned}0 &< x^2 + y^2 \\ &= tp \\ &< 2p^2.\end{aligned}$$

It follows that $x^2 + y^2 = p$.
(b) If $p = 2$ then take $x = 0$ and $y = 1$. Otherwise, pick u such that $u^2 \equiv -2 \mod p$. By (1.2) we may find r and s such that

$$us \equiv r \mod p$$

where $0 < s < \sqrt{p}$ and $|r| \leq \sqrt{p}$. If $r > 0$ then let $\lambda = s$ and $\mu = r$. If $r < 0$ then let $\lambda = -s$ and $\mu = r$. As $u(-r) \equiv 2s \mod p$, dividing through by 2, it follows that $\lambda^2 + 2\mu^2 \equiv 0 \mod p$, $0 < \lambda < \sqrt{p}$ and $0 < \mu < \sqrt{p}$. As

$$\begin{aligned}0 &< \lambda^2 + 2\mu^2 \\ &= tp \\ &< 3p^2.\end{aligned}$$

It follows that either $\lambda^2 + 2\mu^2 = p$ or $\lambda^2 + 2\mu^2 = 2p$. In the former case put $x = \lambda$ and $y = \mu$. In the latter case, $\lambda = 2y$ must be even. Let $x = \mu$. Dividing through by 2 we get $2y^2 + x^2 = p$. Either way, we can find x and y such that $x^2 + 2y^2 = p$.

(c) Presumably one should assume that $p > 2$. If $p = 3$ then take $x = 0$ and $y = 1$. Otherwise, pick u such that $u^2 \equiv -3 \mod p$. By (1.2) we may find r and s such that

$$us \equiv r \mod p$$

where $0 < s < \sqrt{p}$ and $|r| \leq \sqrt{p}$. We may assume that r and s are coprime. If $r > 0$ then let $\lambda = s$ and $\mu = r$. If $r < 0$ then let $\lambda = -s$ and $\mu = r$. As $u(-r) \equiv 3s \mod p$, dividing through by 3, it follows that $\lambda^2 + 3\mu^2 \equiv 0 \mod p$, $0 < \lambda < \sqrt{p}$ and $0 < \mu < \sqrt{p}$. As

$$\begin{aligned} 0 &< \lambda^2 + 3\mu^2 \\ &= tp \\ &< 4p^2. \end{aligned}$$

It follows that either $\lambda^2 + 3\mu^2 = p$ or $\lambda^2 + 3\mu^2 = 2p$ or $\lambda^2 + 3\mu^2 = 3p$. In the second case if one of λ or μ is even then so is the other, a contradiction. Thus we may assume that λ and μ are both odd. Reducing modulo 4 and as p is odd, we get

$$1 + 3 \equiv 2 \mod 4,$$

a contradiction. Thus the second case does not occur.
In the first case put $x = \lambda$ and $y = \mu$. In the third case, $\lambda = 3y$ must be divisible by 3. Let $x = \mu$. Dividing through by 3 we get $3y^2 + x^2 = p$. Either way, we can find x and y such that $x^2 + 3y^2 = p$.
(d) -5 is a residue of 7. Indeed, $3^2 = 9 \equiv -5 \mod 7$. But $x^2 + 5y^2$ is never equal to 7. Indeed, $y \leq 1$. If $y = 0$ we want $x^2 = 7$, impossible. If $y = 1$ we want $x^2 = 2$ also impossible.
More generally, consider primes q congruent to 1 modulo 4. Pick an integer a such that a is not a quadratic residue of q. Let $p > q$ be a prime congruent to 3 modulo 4 and to a modulo q (infinitely many primes p and q exist by Dirichlet's theorem). As q is congruent to one modulo 4, by quadratic reciprocity we have

$$\begin{aligned} \left(\frac{-q}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{q}{p}\right) \\ &= -1\left(\frac{p}{q}\right) \\ &= -1\left(\frac{a}{q}\right) \\ &= 1. \end{aligned}$$

Thus $-q$ is a residue of p.

However, if $x^2 + qy^2 = p$ then consider reducing modulo 4. We get

$$x^2 + y^2 \equiv 3 \mod 4,$$

impossible.
(e) Let $\alpha = a + b\sqrt{2}i$ and $\beta = c + d\sqrt{2}i$. Let

$$N(\alpha) = a^2 + 2b^2.$$

Note that

$$N(\alpha) = \alpha\bar{\alpha}.$$

We have

$$\begin{aligned} N(\alpha\beta) &= (\alpha\beta)\overline{\alpha\beta} \\ &= \alpha\overline{\alpha}\beta\overline{\beta} \\ &= N(\alpha)N(\beta). \end{aligned}$$

Similar calculations pertain, replacing $\sqrt{2}$ by $\sqrt{3}$.
Thus the set of numbers which are of the form $x^2 + 2y^2$, or $x^2 + 3y^2$, are closed under multiplication.
Thus every natural number n such that every -2 is a residue of every prime p dividing is of the form x^2+2y^2. Similarly every natural natural number n such that every -3 is a residue of every odd prime p dividing and which is divisible by a power of 4, is of the form $x^2 + 3y^2$.
7.2.3. As N is odd we may assume that a and c are odd and b and d are even. Let

$$u = (a - c, d - b) \qquad \text{and} \qquad v = (a + c, b + d).$$

Then

$$a - c = lu \qquad \text{and} \qquad d - b = mu,$$

for coprime integers l and m. Note that as

$$a^2 + b^2 = c^2 + d^2 \qquad \text{it follows that} \qquad a^2 - c^2 = b^2 - d^2.$$

Factoring both sides, we get

$$(a - c)(a + c) = (b - d)(b + d).$$

It follows that

$$l(a + c) = m(b + d).$$

As l and m are coprime it follows that

$$(a + c) = m\alpha \qquad \text{and} \qquad b + d = l\beta.$$

Cancelling we see that $\alpha = \beta$ is the greatest common divisor v. Thus

$$(a + c) = mv \qquad \text{and} \qquad b + d = lv.$$

Note that u and v are even. We have

$$\begin{aligned}\left[\left(\frac{u}{2}\right)^2 + \left(\frac{v}{2}\right)^2\right](m^2+l^2) &= \left(\frac{mu}{2} + \frac{lv}{2}\right)^2 + \left(\frac{lu}{2} - \frac{mv}{2}\right)^2 \\ &= \left(\frac{d-b}{2} + \frac{b+d}{2}\right)^2 + \left(\frac{a-c}{2} - \frac{a+c}{2}\right)^2 \\ &= d^2 + c^2 \\ &= N.\end{aligned}$$

7.2.4. It is expedient to find another way to write $1,000,009$ as a sum of squares. This is easy,

$$1,000,009 = 3^2 + (1,000)^2.$$

In this case,

$$a = 235 \qquad b = 972 \qquad c = 3 \qquad \text{and} \qquad d = 1,000.$$

Therefore

$$\begin{aligned}u &= (232, 28) \\ &= 2(116, 14) \\ &= 4(58, 7) \\ &= 4.\end{aligned}$$

and

$$\begin{aligned}v &= (238, 1972) \\ &= 2(119, 986) \\ &= 2 \cdot 17(7, 58)) \\ &= 34.\end{aligned}$$

We have

$$232 = 4 \cdot l$$

so that $l = 58$ and

$$28 = 4m$$

so that $m = 7$. Thus

$$\begin{aligned}1,000,009 &= (2^2 + 17^2)(7^2 + 58^2) \\ &= 293 \cdot 3413.\end{aligned}$$

7.3.1. Suppose that $p \in \mathbb{Z}$ is a prime. If $p = a^2 + b^2$ then $p = (a+bi)(a-bi)$. As

$$N(a+bi) = a^2 + b^2 = p,$$

a prime integer it follows that $a+bi$ is a prime in the Gaussian integers. The associates of $a+bi$ are $a+bi$, $-b+ai$, $-a-bi$ and $b-ai$. The associates of $a-bi$ are the conjugates of these. All eight complex numbers give the same way to write p as a sum of squares.
As $\mathbb{Z}[i]$ is a UFD, there is then only one way to write p as a sum of squares.