Number Theory 2

zc231

1. $1, 1, 1, 1$.

2. $p = 3, 7$ works. For $p \neq 3, 5$ we need $\left(\frac{21}{p}\right) = 1$ and so $\left(\frac{p}{3}\right)\left(\frac{p}{7}\right) = \left((-1)^{\frac{p-1}{2}}\right)^2 = 1$ (or you simply compute this as a Jacobi symbol) and so $\left(\frac{p}{3}\right) = \left(\frac{p}{7}\right) = 1$ which gives $p \equiv 1, 4, 16 \bmod 21$ or $\left(\frac{p}{3}\right) = \left(\frac{p}{7}\right) = -1$ which gives $p \equiv 5, 17, 20 \bmod 21$.

3. If $2^n - 1$ is a prime then n is a prime and since $n > 2$ so n is odd. Therefore $2^n - 1 \equiv 1 \bmod 3$. By reciprocity law
$$\left(\frac{3}{2^n - 1}\right) = -\left(\frac{2^n - 1}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

4. The number of quadratic residues is equal to the number of non-residues, and so there are $\frac{p-1}{2}$ quadratic residues. When $p \equiv 1 \bmod 4$, x is a quadratic residue if and only if $p - x$ is. Therefore there are exactly $\frac{p-1}{4}$ pairs of quadratic residues where the sum of each pair is p. Similarly there are $\frac{p-1}{4}$ pairs of quadratic non-residues where the sum of each pair is p.

   This does not hold for $p \equiv 3 \bmod 4$. For example when $p = 3$ the only quadratic residue is 1 and the only non-residue is 2.

5. Since $\left(\frac{0}{p}\right) = 0$ so we can write $\tau = \sum_{a=0}^{p-1}\left(\frac{a}{p}\right)\zeta^a$.
$$\tau^2 = \sum_{a=0}^{p-1}\left(\frac{a}{p}\right)\zeta^a \sum_{b=0}^{p-1}\left(\frac{b}{p}\right)\zeta^b = \sum_{a=1}^{p-1}\sum_{b=0}^{p-1}\left(\frac{ab}{p}\right)\zeta^{a+b}$$
   because when $a = 0$ the sum $\sum_{b=0}^{p-1}\left(\frac{ab}{p}\right)\zeta^{a+b} = 0$. Now let $i = a + b \pmod p$ so $b = i - a$, and so we have
$$\tau^2 = \sum_{a=1}^{p-1}\sum_{i=0}^{p-1}\left(\frac{ai - a^2}{p}\right)\zeta^i = \sum_{a=1}^{p-1}\sum_{i=0}^{p-1}\left(\frac{a^2}{p}\right)\left(\frac{ia^{-1} - 1}{p}\right)\zeta^i = \sum_{a=1}^{p-1}\sum_{i=0}^{p-1}\left(\frac{ia^{-1} - 1}{p}\right)\zeta^i.$$
   Write $ia^{-1} - 1 = j$ and for each $a \neq 0$, the map $\{0, 1, \ldots, p-1\} \to \{0, 1, \ldots, p-1\}$ by sending i to j is a bijection and $i = a(j + 1)$, so
$$\tau^2 = \sum_{a=1}^{p-1}\sum_{j=0}^{p-1}\left(\frac{j}{p}\right)\zeta^{a(j+1)} = \sum_{j=0}^{p-1}\left(\frac{j}{p}\right)\sum_{a=1}^{p-1}\zeta^{a(j+1)}.$$
   For each $j \neq p - 1$ we see $\sum_{a=1}^{p-1}\zeta^{a(j+1)} = \sum_{k=1}^{p-1}\zeta^k = -1$ because the map $\{0, 1, \ldots, p-1\} \to \{0, 1, \ldots, p-1\}$ by sending a to k is a bijection when $j \neq p - 1$ as the inverse of $(j + 1)$ exists. When $j = p - 1$ we have $\sum_{a=1}^{p-1}\zeta^{ap} = p - 1$. Therefore we conclude
$$\tau^2 = \sum_{j=0}^{p-2}\left(\frac{j}{p}\right)(-1) + \left(\frac{p-1}{p}\right)(p-1) = \left(\frac{-1}{p}\right) + \left(\frac{p-1}{p}\right)(p-1) = p\left(\frac{-1}{p}\right)$$

and so τ^2 is p when $p \equiv 1 \bmod 4$ and $-p$ when $p \equiv 3 \bmod 4$.

Alternatively, note that the sum $\sum_{s=0}^{p-1} \zeta^{rs}$ is p if $r \equiv 0 \bmod p$ and 0 otherwise. Let Q_1 be the set of quadratic residue mod p and Q_2 be the set of quadratic non-residue mod p. Then note that $1+\zeta+\zeta^2+\cdots+\zeta^{p-1} = 0$ and so $1+\sum_{x\in Q_1}\zeta^x+\sum_{y\in Q_2}\zeta^y = 0$ and so $\sum_{y\in Q_2}\zeta^y = -1-\sum_{x\in Q_1}\zeta^x$. So we have

$$\tau = \sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\zeta^a = \sum_{x\in Q_1}\zeta^x - \sum_{y\in Q_2}\zeta^y = 1 + 2\sum_{x\in Q_1}\zeta^x = \sum_{m=0}^{p-1}\zeta^{m^2}$$

because for each $x \in Q_1$ there are exactly two m such that $m^2 = x$. So if $\bar{\tau}$ is the complex conjugate of τ then

$$\tau\bar{\tau} = \sum_{m=0}^{p-1}\zeta^{m^2}\sum_{n=0}^{p-1}\zeta^{n^2} = \sum_{m=0}^{p-1}\zeta_{n=0}^{p-1}\zeta^{(m-n)(m+n)} = \sum_{r=0}^{p-1}\sum_{s=0}^{p-1}\zeta^{rs} = p$$

because for each r, s there exists unique m, n such that $m-n \equiv r \bmod p$ and $m+n \equiv s \bmod p$. Finally, if $p \equiv 1 \bmod 4$ then $x \in Q_1$ if and only if $-x \in Q_1$ so by using $\tau = \sum_{x\in Q_1}\zeta^x - \sum_{y\in Q_2}\zeta^y$ we see $\bar{\tau} = \tau$ so τ is real and so $\tau^2 = \tau\bar{\tau} = p$. If $p \equiv 3 \bmod 4$ then $x \in Q_1$ if and only if $-x \in Q_2$ so $\bar{\tau} = -\tau$ and so τ is purely imaginary, in which case $\tau^2 = -\tau\bar{\tau} = -p$.

6. Let $a = b^2\prod_j q_j 2^\epsilon$ where $q_1, \ldots$ are distinct odd prime, $\epsilon = 0$ or 1 and $q_i \nmid b$ for any b (write a as the product of the squared part and square free part). We will firstly construct one such prime p. Let m be an integer which satisfies the following

$$m \equiv 1 \bmod 8, m \equiv c \bmod q_1 \text{ where } \left(\frac{c}{q_1}\right) = -1, m \equiv 1 \bmod q_i, i \neq 1.$$

Then by reciprocity law (as we pick $m \equiv 1 \bmod 8$) we have

$$\left(\frac{a}{m}\right) = \left(\frac{2^\epsilon}{m}\right)\left(\frac{b^2}{m}\right)\prod_i\left(\frac{q_i}{m}\right) = \prod_i\left(\frac{m}{q_i}\right) = -1$$

by our choice of m. This shows that there exists a prime factor p of m such that $\left(\frac{a}{p}\right) = -1$. In fact, we see that given each m satisfying the above condition, there exists $p\big|m$ such that $\left(\frac{a}{p}\right) = -1$ and so suppose we only have finitely many such p, say $p_1, \ldots, p_r$. Then we take m satisfying the above condition and the additional condition that $m \equiv 1 \bmod p_1\cdots p_r$. Such m exists because $\left(\frac{a}{p_i}\right) = -1$ and so $p_i \nmid a$. In particular $p_i \neq q_j$ for all i, j. Now by construction m is coprime to p_i for each i and then the prime factor $p\big|m$ with $\left(\frac{a}{p}\right) = -1$ is different from $p_1, \ldots, p_r$.

7. $p \equiv 3 \bmod 4$ so -1 is not a square mod p. The map $\{(p+1)/2, \ldots, p-1\} \to \{1, \ldots, (p-1)/2\}$ by sending a to $p-a$ is a bijection. So

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

which gives the first equality. For the second equality, we consider

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

where the first term is the sum over all even numbers less than p and the second one is the sum over odd numbers less than p, and since $p \equiv 3 \bmod 8$ so 2 is not a square but -2 is a square so

$$\sum_{a=1}^{p-1} a\left(\frac{a}{p}\right) = \sum_{a=1}^{(p-1)/2} -2a\left(\frac{a}{p}\right) + (p-2a)\left(\frac{a}{p}\right) = \sum_{a=1}^{(p-1)/2} (p-4a)\left(\frac{a}{p}\right).$$

Now if $p > 3$ then $2p$ is coprime to 3 and so it suffices to show

$$\sum_{a=1}^{(p-1)/2} 2p\left(\frac{a}{p}\right) \equiv 0 \bmod 3.$$

But by the previous part,

$$\sum_{a=1}^{(p-1)/2} (2a-p)\left(\frac{a}{p}\right) = \sum_{a=1}^{(p-1)/2} (p-4a)\left(\frac{a}{p}\right)$$

and we rearrange the equation so

$$\sum_{a=1}^{(p-1)/2} 2p\left(\frac{a}{p}\right) = \sum_{a=1}^{(p-1)/2} 6a\left(\frac{a}{p}\right)$$

in particular $\sum_{a=1}^{(p-1)/2} 2p\left(\frac{a}{p}\right)$ is divisible by 3.

8. No they have different discriminant. No, observe

$$15x^2 - 15xy + 4y^2 \equiv y^2 \bmod 3, 3x^2 + 9xy + 8y^2 \equiv 2y^2 \bmod 3$$

so the first one represents some integer which is 1 mod 3 (by picking $x = 0, y = 1$ etc.) and the second one cannot represent any integer which is 1 mod 3.

9. This becomes obvious if we write each binary quadratic form in terms of $(x,y)A(x,y)^T$ for some 2×2 symmetric matrix A.

10. $d = 8, \langle 1,0,2\rangle$. $d = 11, \langle 1,1,3\rangle$. $d = 12, \langle 1,0,3\rangle, \langle 2,0,2\rangle$. $d = 16, \langle 1,0,4\rangle$. $d = 19, \langle 1,1,5\rangle$. $d = 23, \langle 1,1,6\rangle, \langle 2,1,3\rangle, \langle 2,-1,3\rangle$. $d = 163, \langle 1,1,41\rangle$.

11. The reduced form is $2x^2 - xy + 4y^2$ so the smallest 3 positive integers it represent are $2, 4, 5$.

12. Suppose $p = x^2 + 3y^2$ then $p = 3$ or $p \equiv 1 \bmod 3$. Conversely, we know an integer p is represented by a form of discriminant d if and only if $x^2 \equiv d \bmod 4p$ is solvable. We know $p = 2$ is not represented by $x^2 + 3y^2$ so we assume $p \geq 3$. We see the only primitive (meaning the coefficients have greatest common divisor 1) reduced form of discriminant -12 is $x^2 + 3y^2$. So we want either $p = 3$ or by CRT $x^2 \equiv -12 \bmod 4$ and $x^2 \equiv -12 \bmod p$ are both solvable which is equivalent to

$$\left(\frac{-12}{p}\right) = \left(\frac{-3}{p}\right) = 1$$

but this is equal to $\left(\frac{p}{3}\right)$ by reciprocity law and so it is equivalent to $p \equiv 1 \bmod 3$.

13. The first one is x^2+2y^2. It represents 2 and it is the only reduced form of discriminant -8 and a prime is represented by a form of discriminant -8 if and only if $\left(\frac{-2}{p}\right)=1$, if and only if $p\equiv 1,3 \bmod 8$. The second one is x^2+y^2 and we check it works by the same argument. For the last one, there does not exist such a binary form. If it exists then we may assume it is reduced, and it represents $2,7$ but it does not represent $3,5$ so consider the possible reduced form which represent $2,7$ but not $3,5$

$$f_1=\langle 2,\pm 1,7\rangle, f_2=\langle 2,0,7\rangle$$

using the fact that the smallest integers represented by a reduced form $ax^2+bxy+cy^2$ are $a,c,a+c-b$. Then we see f_1 represents 43 ($x=4,y=1$) which is not $1,7 \bmod 8$ and f_2 does not represent 17.

14. These two are the only reduced forms of discriminant -15 so n is represented by one of them if and only if $x^2\equiv -15 \bmod 4n$ is solvable. Write $n=2^a3^b5^c\prod_i p_i^{e_i}$ where $p_i\neq 3,5$ and so we require, by CRT

$$x^2\equiv -15 \bmod 2^a, x^2\equiv -15 \bmod 3^b, x^2\equiv -15 \bmod 5^c, x^2\equiv -15 \bmod p_i^{e_i}$$

are all solvable.

By Hensel's Lemma (or using the proof of Hensel's Lemma) $x^2\equiv -15 \bmod 2^n, n\geq 3$ is always solvable and so $a\geq 0$. It is clear that $x^2\equiv -15 \bmod 9$, $x^2\equiv -15 \bmod 25$ are not solvable so $b,c\leq 1$. Finally, if $p\neq 2,3,5$ then by Hensel's Lemma we require $\left(\frac{-15}{p}\right)=1$ which then implies $p\equiv 1,2,4,8 \bmod 15$. This classifies the possible prime factors (and their indices) of n. If now n is prime to 15, if $n=x^2+xy+4y^2$ then $n\equiv x^2-2xy+y^2=(x+y)^2 \bmod 3$ so $n\equiv 1 \bmod 3$. If $n=2x^2+xy+2y^2$ then $n\equiv -x^2-2xy-y^2=-(x+y)^2 \bmod 3$ so $n\equiv -1 \bmod 3$.

In case he doesn't cover Hensel's Lemma in this course, here is something useful. Let $p\geq 3$ be a prime, and a an integer coprime to p, then $\left(\frac{a}{p}\right)=1$ if and only if $x^2\equiv a \bmod p^n$ is solvable for all n. To prove this, one direction is obvious and so we assume $\left(\frac{a}{p}\right)=1$ so $x^2\equiv a \bmod p$ is solvable. Suppose we have a solution to $x^2\equiv a \bmod p^n$, then $x^2=a+p^nb$ for some integer b. Then let $y=x+p^nt$ and so

$$y^2=x^2+2p^ntx+p^{2n}t^2=a+p^n(b+2tx)+p^{n+1}p^{n-1}t^2\equiv a+p^n(b+2tx) \bmod p^{n+1}.$$

Since $(a,p)=1$ so $(x,p)=1$ and as $p>2$ so $(2x,p)=1$. In particular $(2x)^{-1}$ exists in $(\mathbb{Z}/p\mathbb{Z})^\times$. Therefore, take $t\equiv b(2x)^{-1} \bmod p$ we obtain a solution y such that $y^2\equiv a \bmod p^{n+1}$. By induction, this shows that $x^2\equiv a \bmod p^n$ has a solution for all n. Another way to see this is, since $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is cyclic, pick a generator g for the group. If a is not a square then $a=g^{2k+1}$ for some k. But g is also a generator for $(\mathbb{Z}/p\mathbb{Z})^\times$ so $a=g^{2k+1}$ where now both a,g are considered as elements in $(\mathbb{Z}/p\mathbb{Z})^\times$ and this shows a is not a square mod p, which is a contradiction.

The statement for $p=2$ is similar. Let a be an odd number, then a is a square mod 8 if and only if a is a square mod $2^n, n\geq 3$. Again you can show this by induction, suppose $x^2\equiv a \bmod 2^n$, so $x^2=a+2^nb$ for some b. Take $y=x+2^{n-1}t$ then

$$y^2=x^2+2^ntx+2^{2n-2}t^2=a+2^n(b+tx)+2^{n+1}2^{n-3}t^2\equiv a+2^n(b+tx) \bmod 2^{n+1}$$

because $n\geq 3$ and since a is odd so x must be odd and so take t which has the same parity as b we se $y^2\equiv a \bmod 2^{n+1}$.