# Solutions to Exercises in Cassels Lectures on Elliptic Curves

Yankı Lekili

## Chapter 0

No exercises given.

## Chapter 1

No exercises given.

## Chapter 2

**1)** For each sets of $p$,$m$,$r$ given, either find an $x \in \mathbb{Z}$ such that

$$|r - x|_p \leq p^{-m}$$

or show that no such $x$ exists.

(i) $p = 257$, $r = 1/2$, $m = 1$;

▶ $|\frac{1}{2} - x| \leq 257^{-1}$ if and only if $257 \mid 2x - 1$. So, take $x = 258/2 = 129$.

(ii) $p = 3$, $r = 7/8$, $m = 2$;

▶ $|\frac{7}{8} - x| \leq 3^{-2}$ if and only if $9 \mid 8x - 7$. So, take $x = 2$.

(iii) $p = 3$, $r = 7/8$, $m = 7$;

▶ $|\frac{7}{8} - x| \leq 3^{-7}$ if and only if $3^7 \mid 8x - 7$. We try to solve $8x = 7(3^i)$ order by order for $i = 2, \ldots, 7$. For $i = 2$, the previous exercise gives 2 is a solution, so let's write $x = 2 + 3^2 a_2 + 3^3 a_3 + 3^4 a_4 + 3^5 a_5 + 3^6 a_6$ for $a_i \in \{0, 1, 2\}$. $8.2 - 7 = 9$ so to solve $8x = 7(27)$ we need a non-zero $a_2$. We try $a_2 = 1$ and get $8.(2 + 9) - 7 = 81 \equiv 0(81)$, hence we can take $x = 2 + 3^2 + 3^4 a_4 + 3^5 a_5 + 3^6 a_6$. We try $a_4 = 1$, then $8(2 + 9 + 81) - 7 = 729 = 3^6$. Hence, we get $x = 2 + 9 + 81 + 729$. Finally, let us try $a_6 = 1$, we compute $729 + 8.729 = 9.729 = 3^8$. So, take $x = 821$.

(iv) $p = 3$, $r = 5/6$, $m = 9$;

▶ $|\frac{5}{6} - x| \leq 3^{-9}$ if and only if $3^{10} \mid 6x - 5$ (since $3 \mid 6$). But, this is impossible since $6x - 5 \equiv 2(3)$.

(v) $p = 5$, $r = 1/4$, $m = 4$;

▶ $|\frac{1}{4} - x| \leq 5^{-4}$ if and only if $5^4 \mid 4x - 1$.

Let's try to solve $4x \equiv 1(5^i)$ for $i = 1, 2, 3, 4$. Write $x = a_0 + 5a_1 + 5^2a_2 + 5^3a_3$ with $a_i \in \{0, 1, 2, 3, 4\}$. We can easily see $a_0 = 4$ solves $4x \equiv 1(5)$. Next, we try $4.(4 + 5a_1) \equiv 1(25)$. This reduces to $20a_1 \equiv 10(25)$, which has a solution $a_1 = 3$. Next, we have $4.(4+5.3+25a_2) \equiv 1(125)$ which reduces to $100a_2 = 50(125)$. So, take $a_2 = 3$. Finally, we have $4.(4+5.3+25.3+125.a_3) \equiv 1(625)$ which is equivalent to $500a_3 = 250(625)$. Hence, $a_3 = 3$. So, take $x = 4 + 5.3 + 25.3 + 125.3 = 469$.

**2)** Construct further examples along the lines of Exercise 1 until the whole business seems trivial.

▶ Take $p = 57$, just kidding.

**3)** For given $p, m, r$ either find an $x \in \mathbb{Z}$ such that

$$|r - x^2|_p \leq p^{-m}$$

or show that no such $x$ exists.

(i) $p = 5$, $r = -1$, $m = 4$;

▶ $| - 1 - x^2|_p \leq 5^{-4}$ if and only if $5^4|x^2 + 1$. Let's try $x = a_0 + a_15 + a_25^2 + a_35^3$. We need $a_0^2 + 1 \equiv 0(5)$. There are two solutions to this: $a_0 = 2, 3$. We look for solutions of the form $x_0 = 2 + a_15 + a_25^2 + a_35^3$ and $x_1 = 3 + b_15 + b_25^2 + b_35^3$. Next, we need to solve $(2 + a_15)^2 + 1 \equiv 0(25)$ and $(3 + b_15)^2 + 1 \equiv 0(25)$. We get $5 + 20a_1 \equiv 0(25)$ and $10 + 30b_1 \equiv 0(25)$. Thus, $a_1 = 1$ and $b_1 = 3$. Next, we solve $(2 + 1.5 + a_25^2)^2 + 1 \equiv 0(125)$ and $(3 + 3.5 + b_25^2)^2 + 1 \equiv 0(125)$. We get $50 + 100a_2 \equiv 0(125)$ and $75 + 25b_2 \equiv 0(125)$. Thus, $a_2 = 2$ and $b_2 = 2$. Finally, we look for solutions to $(2 + 1.5 + 2.5^2 + a_35^3)^2 + 1 \equiv 0(125)$ and $(3 + 3.5 + 2.5^2 + b_35^3)^2 + 1 \equiv 0(125)$. Expanding these, we find $125 + 500a_3 \equiv 0(625)$ and $250 + 125b_3 \equiv 0(625)$, so $a_3 = 1$ and $b_3 = 3$. Therefore, the solutions are

$$2 + 1.5 + 2.5^2 + 1.5^3, \quad 3 + 3.5 + 2.5^2 + 3.5^3$$

(ii) $p = 5$, $r = 10$, $m = 3$;

▶ $|10 - x^2|_p \leq 5^{-3}$ if and only if $5^3 \mid x^2 - 10$. This means $5|x^2$ but that implies $25|x^2$. However $25 \nmid 10$, therefore, there is no solution to this with $x \in \mathbb{Z}$.

(iii) $p = 13$, $r = -4$, $m = 3$;

▶ $| - 4 - x^2|_p \leq 13^{-3}$ if and only if $13^3 \mid x^2 + 4$.

We see easily that $3^2+4 \equiv 0(13)$ so let's try $x = 3+a_113+a_213^2$. Then, we get $(3+13a_1)^2+4 \equiv 0(13^2)$. Hence, $13 + 78a_1 \equiv 0(169)$, so $a_1 = 2$. Then, we need to solve $(3 + 2.13 + a_2.13^2)^2 + 4 \equiv 0(13^3)$. This gives $5.13^2 + a_258.13^2 \equiv 0(13^3)$, hence $a_2 = 10$. So, take $x = 3 + 2.13 + 10.13^2$. There is another solution if you try $x = 10 + b_113 + b_213^2$. and working this out gives another solution $x = 10 + 10.13 + 2.13^2$.

(iv) $p = 2$, $r = -7$, $m = 6$;

► $|-7-x^2|_p \leq 2^{-6}$ if and only if $2^6 \mid x^2+7$.

We try out $x = 1+2a_1+2^2a_2+2^3a_3+2^4a_4+2^5a_5$ for $a_i \in \{0,1\}$. If we square this, we see that whether $a_5 = 0$ or 1 does not matter, therefore, we can take $a_5 = 0$. Let's consider modulo 32, then by a similar reason whether $a_4 = 0$ or 1 doesn't matter, so let's consider the equation:

$$(1+2a_1+2^2a_2+2^3a_3)^2+7 \equiv 0(32)$$

We see that this is equivalent to $(1+2a_1+4a_2)^2+16a_3+7 \equiv 0(32)$. Let's now reduce to modulo (16), then we get the equation

$$(1+2a_1)^2+8a_2+7 \equiv 0(16)$$

Now, by inspection, we can see that the only solutions are $a_1 = 1, a_2 = 0$ or $a_1 = 0, a_2 = 1$. Getting back to the modulo (32) equation, we get that the only solutions are $a_1 = 1, a_2 = 0, a_3 = 1$ or $a_1 = 0, a_2 = 1, a_3 = 0$. Finally, we want to see if either of these can be extended to the solution of the original problem for some $a_4 \in \{0,1\}$. We try $x = 1+2.1+8.1+16a_4$ and $x = 1+4.1+16a_4$ for $a_4 \in \{0,1\}$. In the first case, we get $x^2+7 \equiv 128+32a_4(64)$ and in the second case we get $x^2+7 = 32+32a_4(64)$ and we see that the latter one gives the solution: $x = 1+4.1+16.1 = 21$.

(v) $p = 7$, $r = -14$, $m = 4$;

► $|-14-x^2|_p \leq 7^{-4}$ if and only if $7^4 \mid x^2+14$.

It follows that $7 \mid x$ but then $7^2 \mid x^2$. Now, we arrive at contradiction, because $7^4 \mid x^2+14$, in particular implies $7^2 \mid x^2+14$ and this together with $7^2 \mid x^2$ implies $7^2 \mid 14$ which is false.

(vi) $p = 7$, $r = 6$, $m = 3$;

► $|6-x^2|_p \leq 7^{-3}$ if and only if $7^3 \mid x^2-6$.

No solution because there is no $x \in \mathbb{Z}$ such that $x^2-6$ is divisible by 7 as can be easily checked by trying out $x = 0,1,2,3,4,5,6$.

(vii) $p = 7$, $r = 1/2$, $m = 3$;

► $|\frac{1}{2}-x^2|_p \leq 7^{-3}$ if and only if $7^3 \mid 2x^2-1$.

Looking modulo 7, we see we have $x = 2+7a_1+7^2a_2$ or $x = 5+7b_1+7^2b_2$ are possible solution. We then look at modulo $7^2$, we get $7^2 \mid 7+7a_1$ and $7^2 \mid 28b_1$, so we take $a_1 = 6$ and $b_1 = 0$. Finally, $7^3 \mid 2(2+7.6+7^2a_2)^2-1$ gives $7^3 \mid 2.7^2+a_27^2$, hence $a_2 = 5$. Similarly, $7^3 \mid 2(5+7^2b_2)^2-1$ gives $7^3 \mid 7^2+6b_27^2$, thus $b_2 = 1$. We conclude that $2+7.6+7^2.5$ and $5+7^2.1$ are the desired solutions.

**4)** As in Exercise 2.

► Solution as in Exercise 2.

**5)** Let $p > 0$ be a prime, $p \equiv 2(3)$. For any integer $a, p \nmid a$, show that there is an $x \in \mathbb{Z}_p$ with $x^3 = a$.

► Consider the group homomorphism $x \to x^3$ from $\mathbb{F}_p^\times$ to itself. Since $3 \nmid p-1$, there are no order 3 elements in $\mathbb{F}_p^\times$. Therefore, this map is injective, hence also surjective. This means that we can find $x_1$ with $x_1^3 \equiv a(p)$. Next, suppose that we have $x_n^3 \equiv a(p^n)$ and pose $x_{n+1} = x_n + p^n y$ and we seek to solve $x_{n+1}^3 \equiv a(p^{n+1})$. We compute $x_{n+1}^3 = (x_n + p^n y)^3 \equiv x_n^3 + 3p^n x_n^2 y(p^{n+1})$. As by assumption $p^n \mid x_n^3 - a$, if we let $y$ such that $3x_n^2 y = \frac{x_n^3 - a}{p^n}(p)$ (which we can do since $p \nmid 3x_n^2$, as $p \nmid a$ and $p \neq 3$), then $p^{n+1} \mid x_{n+1}^3 - a$ as required.

# Chapter 3

**6)** (i) Let $p > 2$ prime and let $b, c \in \mathbb{Z}$, $p \nmid b$. Show that $bx^2 + c$ takes precisely $\frac{1}{2}(p+1)$ distinct values mod $p$ for $x \in \mathbb{Z}$.

► It suffices to show the special case $b = 1, c = 0$, since $bm + c \equiv bn + c(p)$ implies $m \equiv n(p)$ as $p \nmid b$. Now, $x^2 \equiv y^2(p)$ then $(x-y)(x+y) \equiv 0(p)$, hence $x \equiv y(p)$ or $x \equiv -y(p)$. Therefore, the map $x \to x^2(p)$ is two-to-one except at 0, so the number of elements in the image is $1 + \frac{p-1}{2} = \frac{p+1}{2}$.

(ii) Suppose that, further, $a \in \mathbb{Z}$, $p \nmid a$. Show that there are $x, y \in \mathbb{Z}$ such that $bx^2 + c \equiv ay^2(p)$.

► The sets of elements of the form $bx^2 + c$ and $ay^2$ both contain $\frac{p+1}{2}$ elements since $\frac{p+1}{2} + \frac{p+1}{2} > p$, these sets have to overlap.

**7)** Let $a, b, c \in \mathbb{Z}_p$, $|a|_p = |b|_p = |c|_p = 1$ where $p$ is prime, $p > 2$. Show that there are $x, y \in \mathbb{Z}_p$ such that $bx^2 + c = ay^2$.

► From the previous exercise, we know that there is a solution $(x_1, y_1)$ modulo $p$. Suppose $(x_n, y_n)$ satisfy $bx_n^2 + c \equiv ay_n^2(p^n)$. Let $x_{n+1} = x_n + p^n u$ and $y_{n+1} = y_n + p^n v$. Then, we want to solve $bx_n^2 + 2bx_n p^n u + c \equiv ay_n^2 + 2ay_n p^n v(p^{n+1})$. This boils down to solving $2bx_n u - 2ay_n v \equiv \frac{ay_n^2 - bx_n^2 - c}{p^n}(p)$. This can be solved as long as $p$ does not divide both $x_n$ and $y_n$ and we know that because $|c|_p = 1$.

**8)** Let $p > 2$ be prime, $a_{ij} \in \mathbb{Z}$ $(1 \leq i, j \leq 3)$, $a_{ji} = a_{ij}$ and let $d = \det(a_{ij})$. Suppose that $p \nmid d$. Show that there are $x_1, x_2, x_3 \in \mathbb{Z}$ not all divisible by $p$, such that $\sum_{i,j} a_{ij} x_i x_j = 0(p)$.

► Suppose $a_{ij} = a_{ji} \neq 0$, make a $\mathbb{Z}$-linear change of co-ordinates by sending $x_i \to x_i - a_{ij} x_j$ to transform $\sum_{i,j} a_{ij} x_i x_j$ to $f_1 x_1^2 + f_2 x_2^2 + f_3 x_3^2$. The condition on $d$ becomes $p \nmid f_1 f_2 f_3$. Take $x_3 = 1$ (or any integer that is not divisible by $p$), then the problem reduces to what we solved in Exercise 1 by letting $f_1 = b$, $x_1 = x$, $f_2 = -a$, $x_2 = y$, $f_3 x_3^2 = c$.

**9)** Let $a, b, c \in \mathbb{Z}$, $2 \nmid abc$. Show that a necessary and sufficient condition that the only solution in $\mathbb{Q}_2$ of $ax^2 + by^2 + cz^2 = 0$ is the trivial one is that $a \equiv b \equiv c(4)$.

► Suppose $(a_1, a_2, a_3) \neq 0$ is a non-trivial solution in $\mathbb{Q}_2$ then we can assume that $\max|a_i|_2 = 1$ by multiplying with an element of $\mathbb{Q}_2$. This means that at least one the $a_i$ is a unit. Now, since $aa_1^2 + ba_2^2 + ca_3^2 = 0$ and $2 \nmid abc$, it follows that precisely two of the $a_j$ are units. Because of the non-archimedean inequality, we must have two of the $|aa_1|^2, |ba_2|^2, |ca_3|^2$ must be equal and the other one is less than or equal to. Suppose, for instance, that $|a_2| = |a_3| = 1$, and $|a_1| \leq 1$. By examining modulo 2, we see then that $|a_1| < 1$. Now, $2 \mid a_1$, hence it follows that $b + c \equiv 0(4)$ but $b, c$ are odd, hence $b$ is not equivalent to $c$ modulo 4.

Conversely, suppose that $(a, b, c) \neq (1, 1, 3)$ or $(1, 3, 3)$ modulo 4, and we want to construct a solution in $\mathbb{Q}_2$. By multiplying the equation with $-1$, we can assume that we are in the case where $(a, b, c) = (1, 1, 3)$ modulo 4, or equivalently we are interested in the equation $ax^2+by^2 = (-c)z^2$. Now, multiply both sides with $-(1/c)$ to and redefine $a, b$ to reduce to the case $ax^2 + by^2 = z^2$ where we still have $(a, b) = (1, 1)$ modulo 4. We now appeal to Lemma 4 from Chapter 2, which says that $ax^2 + by^2$ is a square in $\mathbb{Q}_2$ if and only if $ax^2 + by^2 \equiv 1(8)$. We have that $a, b$ are either 1 or 5 modulo 8. So it suffices to find solutions for the four equations: $x^2 + y^2 \equiv 1(8), 5x^2 + y^2 \equiv 1(8), x^2 + 5y^2 \equiv 1(8), 5x^2 + 5y^2 \equiv 1(8)$. It is very easy to solve these congruence equations. For example $(3, 0), (1, 2), (2, 1), (2, 1)$ are solutions in the respective order.

**10)** For each of the following sets of $a, b, c$ find the set of primes $p$ (including $\infty$) for which the only solution of $ax^2 + by^2 + cz^2 = 0$ in $\mathbb{Q}_p$ is the trivial one:

(i) (a,b,c) = (1,1,-2)

▶ Since the equation is homogeneous for $p \neq \infty$, we may assume that if there is a non-trivial solution $(x, y, z)$, then $x, y, z \in \mathbb{Z}_p$.

We see that $(1, 1, 1)$ is a solution in $\mathbb{Z}$. Therefore, there are non-trivial solutions for every $p$ (including $\infty$).

(ii) (a,b,c) = (1,1,-3)

▶ This is the equation $x^2 + y^2 = 3z^2$. It is easy to obtain solutions over $\mathbb{R}$ such as $(\sqrt{3}, 0, 1)$. There are no non-trivial solutions over $\mathbb{Q}_2$ by the previous exercise since $1 \equiv -3(4)$. There no solutions over $\mathbb{Q}_3$ since the only way $x^2+y^2$ is divisible by 3 is if both $x$ and $y$ are divisible by 3 but that implies $z$ has to be divisible by 3, and continuing this way we see that $|x|_3 = |y|_3 = |z|_3 = 0$, which implies $x = y = z = 0 \in \mathbb{Q}_3$. There are non-trivial solutions over any other prime by Exercise 2.

(iii) (a,b,c) = (1,1,1)

▶ This is the equation $x^2 + y^2 + z^2 = 0$. There are no non-trivial solutions over $\mathbb{R}$ since the left hand side is strictly positive unless $x = y = z = 0$. There are no non-trivial solutions over $\mathbb{Q}_2$ by the previous exercise. There are non-trivial solutions over any other prime by Exercise 2.

(iv) (a,b,c) = (14,-15,33)

▶ This is the equation $14x^2 + 33z^2 = 15y^2$.

There are non-trivial solutions over $\mathbb{R}$: Take, for example, $(15\sqrt{14}, 0, 14\sqrt{15})$. There are non-trivial solutions over $\mathbb{Q}_2$ by the previous exercise, since 14 is not equivalent to 33 modulo 4. By Exercise 2, there are non-trivial solutions over any prime $p > 11$. It remains to the understand the cases $p = 3, 5, 7, 11$.

We see that $|x|_3 < 1$, hence we can write $x = 3\tilde{x}$ with $\tilde{x} \in \mathbb{Z}_3$. We then get the equivalent equation, $42\tilde{x}^2 + 11z^2 = 5y^2$. Multiplying both sides by 5, we get $5.42\tilde{x}^2 + 55z^2 = (5y)^2$. Now, we can appeal to Lemma 3 from Chapter 2, which says that a number is a square in $\mathbb{Q}_3$ if and only if it is over $\mathbb{F}_3$. Reducing mo 3, we get $5.42\tilde{x}^2 + 55z^2 = z^2$. Hence, for any value of $z$, we will get solutions.

$14x^2 + 33z^2 \equiv 4x^2 + 3z^2(5)$. The only way $4x^2 + 3z^2$ is divisible by 5 is if both $x$ and $z$ are divisible by 5 but that implies that $y$ has to be divisible by 5, and continuing this way we see that $|x|_5 = |y|_5 = |z|_5 = 0$, which implies $x = y = z = 0 \in \mathbb{Q}_5$.

$15y^2 - 33z^2 \equiv y^2 + 2z^2(7)$. The only way $y^2 + 2z^2$ is divisible by 7 is if both $y$ and $z$ are divisible by 7 but that implies that $x$ has to be divisible by 7, and continuing this way we see that $|x|_7 = |y|_7 = |z|_7 = 0$, which implies $x = y = z = 0 \in \mathbb{Q}_7$.

If we multiply both sides by 14 we get to the equivalent equation: $(14x)^2 = 14.15y^2 - 14.33z^2$. To see that this has solutions over $\mathbb{Q}_{11}$ we can appeal to Lemma 3 from Chapter 2, which says that a number is a square in $\mathbb{Q}_{11}$ if and only if it is over $\mathbb{F}_{11}$. Reducing mod 11, we get $14.15y^2 - 14.33z^2 = y^2$. Hence, for any non-zero value of $y$, we will get solutions.

**11)** Do you observe anything about the parity of the number $N$ of primes (including $\infty$) for which there is insolubility? If not, construct similar exercises and solve them until the penny drops.

▶ It seems to be always even.

**12)** (i) Prove your observation in (6) in the special case $a = 1, b = -r, c = -s$, where $r, s$ are distinct primes $> 2$. [Hint. Quadratic reciprocity]

▶ This is the equation $x^2 = ry^2 + sz^2$. Given $r, s$ are prime numbers, the only primes where we may not have non-trivial solutions are $p = 2, r, s$. By Exercise 4, there are non-trivial solutions in $\mathbb{Q}_2$ if and only if at least one of $r$ and $s$ is 1 mod (4). As for solutions $\mathbb{Q}_r$ we need to see if $x^2 \equiv sz^2(r)$ is solvable or equivalently whether $s$ is a quadratic residue modulo $r$, and similarly for $\mathbb{Q}_s$ we need to see if $x^2 \equiv ry^2(s)$ is solvable or equivalently whether $r$ is a quadratic residue modulo $s$. The required evenness is now a direct consequence of quadratic reciprocity law which says: If $r$ or $s$ are congruent to 1 modulo 4, then: $x^2 \equiv r(s)$ is solvable if and only if $x^2 \equiv s(r)$ is solvable, and if r and s are congruent to 3 modulo 4, then: $x^2 \equiv r(s)$ is solvable if and only if $x^2 \equiv s(r)$ is not solvable.

(ii) [Difficult.] Prove your observation for all $a, b, c \in \mathbb{Z}$.

▶ This is equivalent to quadratic reciprocity. A proof is given in Cassel's book "Rational quadratic forms" Lemma 3.4.