SUM OF DISTINCT J-INVARIANTS OF EDWARDS ELLIPTIC CURVES OVER FINITE FIELDS

JĘDRZEJ MIARECKI

Abstract. Let $p \geq 5$ be prime and $\mathbb{F}_p$ be a finite field. We denote by $\mathcal{J}_p$ a set of all possible distinct j-invariants of Edwards elliptic curve over a field $\mathbb{F}_p$. In this paper we will show that

$$\sum_{j \in \mathcal{J}_p} j = \begin{cases} 396 \pmod{p} & \text{if } p \equiv 3 \pmod{8}, \\ 424 \pmod{p} & \text{if } p \equiv 1, 5 \pmod{8}, \\ -468 \pmod{p} & \text{if } p \equiv 7 \pmod{8}. \end{cases}$$

This paper is based on a chapter from my bachelor's thesis [3], originally written in Polish.

1. Introduction

The equation of an Edwards elliptic curve over a field $\mathbb{K}$ which does not have characteristic 2 is given by

$$E_d/\mathbb{K}: \; x^2 + y^2 = 1 + dx^2y^2, \tag{1.1}$$

where $d \in \mathbb{K} \backslash \{0, 1\}$. We will only consider Edwards curves over finite fields $\mathbb{K} = \mathbb{F}_p$. For these curves we define their j-invariant as

$$j\left(E_d\right) = \frac{16(1 + 14d + d^2)^3}{d(1-d)^4} \pmod{p}. \tag{1.2}$$

Let $\mathcal{J}_p$ be a set of all possible j-invariants of an Edwards curve over a finite field $\mathbb{F}_p$. For example, if $p = 17$ we have that

$$\mathcal{J}_{17} = \{1, 6, 9, 10, 11, 14, 16\}.$$

Note that some elements d generate the same j-invariant j_d. Continuing our example $p = 17$:

d	j_d
2,9	9
3,6	6
4,13,16	11
5,7	16
8,15	10
10,12	1
11,14	14

In this paper we explore the sum of all the elements of $\mathcal{J}_p$. We will prove the following Theorem

Theorem 1.1. *For all primes $p \geq 5$*

$$S_p = \sum_{j \in \mathcal{J}_p} j \equiv \begin{cases} 396 \pmod{p} & \text{if } p \equiv 3 \pmod{8}, \\ 424 \pmod{p} & \text{if } p \equiv 1,5 \pmod{8}, \\ -468 \pmod{p} & \text{if } p \equiv 7 \pmod{8}, \end{cases} \tag{1.3}$$

that is the sum of distinct j-invariants of an Edwards elliptic curve over $\mathbb{F}_p$ can take three different values depending on $p \pmod 8$. It is also worth looking at the sum of all j-invariants. Specifically

Theorem 1.2. *For any finite field $\mathbb{F}_{p^n}$, where $p \in \mathbb{P}$, $n \in \mathbb{N}$, $p \geq 5$, the following holds:*

$$\sum_{d \in \mathbb{F}_{p^n} \setminus \{0,1\}} j(E_d) = -1504. \tag{1.4}$$

Thus, the sum of all j-invariants in the field $\mathbb{F}_{p^n}$ does not depend on p^n.

Proof. The above theorem follows from the fact that:

$$j(E_d) = 16d + \frac{12288}{d-1} + \frac{77824}{(d-1)^2} + \frac{131072}{(d-1)^3} + \frac{65536}{(d-1)^4} + \frac{16}{d} + 736$$

and from the known [4] properties of the sums of the m-th powers of all elements of $\mathbb{F}_{p^n}$:

$$S^m(p^n) = \sum_{x \in \mathbb{F}_{p^n}} x^m = \begin{cases} -1 & \text{if } m \geq 1 \text{ and } p^n - 1 | m, \\ 0 & \text{otherwise.} \end{cases} \tag{1.5}$$

Specifically, we compute using (1.5):

$$\sum_{d \in \mathbb{F}_{p^n} \setminus \{0,1\}} j(E_d) = \sum_{d \in \mathbb{F}_{p^n} \setminus \{0,1\}} 16d + \sum_{d \in \mathbb{F}_{p^n} \setminus \{0,1\}} \frac{12288}{d-1} + \sum_{d \in \mathbb{F}_{p^n} \setminus \{0,1\}} \frac{77824}{(d-1)^2}$$

$$+ \sum_{d \in \mathbb{F}_{p^n} \setminus \{0,1\}} \frac{131072}{(d-1)^3} + \sum_{d \in \mathbb{F}_{p^n} \setminus \{0,1\}} \frac{65536}{(d-1)^4} + \sum_{d \in \mathbb{F}_{p^n} \setminus \{0,1\}} \frac{16}{d} + \sum_{d \in \mathbb{F}_{p^n} \setminus \{0,1\}} 736$$

$$= (-16) + 12288 + (-77824) + 131072 + (-65536) + (-16) + 2 \cdot (-736) = -1504.$$

⊠

By $\left(\frac{*}{*}\right)_L$ we denote the Legendre symbol, that is:

$$\left(\frac{d}{p}\right)_L = \begin{cases} 1 \text{ if } d \text{ is a quadratic residue modulo } p \\ -1 \text{ if } d \text{ is a quadratic nonresidue modulo } p \\ 0 \text{ if } p | d. \end{cases}$$

Throughout the rest of the paper, we will use its well-known properties.

Lemma 1.3.

$$j(E_d) = \frac{16(1 + 14d + d^2)^3}{d(1-d)^4} \equiv 0 \pmod{p} \iff p \equiv 1, 11 \pmod{12}.$$

Proof. Notice that we obtain 0 if and only if

$$1 + 14d + d^2 \equiv 0 \pmod{p} \iff (d+7)^2 \equiv 48 \pmod{12}.$$

The above congruence has a solution if 48 is a quadratic residue modulo p.

$$\left(\frac{48}{p}\right)_L = 1 \iff \left(\frac{2^4}{p}\right)_L \left(\frac{3}{p}\right)_L = \left(\frac{3}{p}\right)_L = 1.$$

From the properties of quadratic residues, we know that 3 is a quadratic residue modulo p if and only if $p \equiv 1, 11 \pmod{12}$. ☒

Lemma 1.4.

$$j(E_d) = j\left(E_{d^{-1}}\right)$$

Proof. Simple calculation shows that

$$\frac{16(1+14d+d^2)^3}{d(1-d)^4} \equiv \frac{16(1+14d^{-1}+(d^{-1})^2)^3}{d^{-1}(1-d^{-1})^4} \pmod{p}.$$

☒

Lemma 1.5. *For $d \equiv -1 \pmod{p}$ we have*

$$j(E_d) \equiv 1728 \pmod{p}.$$

Proof. Simple calculation. ☒

Lemma 1.6. *For $d \in \mathbb{F}_p \setminus \{0,1\}$ we have*

$$\left(\frac{d}{p}\right)_L = \left(\frac{d^{-1}}{p}\right)_L.$$

Proof.

$$1 = \left(\frac{1}{p}\right)_L = \left(\frac{dd^{-1}}{p}\right)_L = \left(\frac{d}{p}\right)_L \left(\frac{d^{-1}}{p}\right)_L,$$

therefore

$$\left(\frac{d}{p}\right)_L = \left(\frac{d^{-1}}{p}\right)_L = 1 \qquad \text{or} \qquad \left(\frac{d}{p}\right)_L = \left(\frac{d^{-1}}{p}\right)_L = -1.$$

☒

We proceed to the proof of Theorem 1.1. We will consider 4 cases, depending on the value $p \pmod{8}$.

2. Case $p \equiv 3 \pmod{8}$

Since we are summing over the elements of the set $\mathcal{J}_p$ and we know that many values of d can generate the same j-invariant, we first need to examine the structure of the solutions to the following congruence. Additionally, assume that for every d, we have $d^2 + 14d + 1 \not\equiv 0 \pmod{p}$, as this does not change the value of the sum (1.3).

Lemma 2.1. *If for $p \equiv 3 \pmod{8}$ the congruence*

$$\frac{16(1+14d+d^2)^3}{d(1-d)^4} \equiv j_0 \pmod{p},$$

where $j_0 \not\equiv 0 \pmod{p}$ has a solution, then one of the following three cases occurs:

(a) *Two distinct elements d_0, d_0^{-1} are solutions, neither of which is a quadratic residue modulo p. The set of quadratic nonresidues is denoted as QNR.*

(b) *Four distinct elements $d_1, d_1^{-1}, d_2, d_2^{-1}$ are solutions, and all of them are quadratic residues modulo p. The set of quadratic residues is denoted as QR.*

(c) *The element $d = p-1$ is the only solution for which $j_0 \equiv 1728 \pmod{p}$.*

Proof of Lemma 2.1. (a) Consider the congruence

$$\frac{(1+14x+x^2)^3}{x(1-x)^4} \equiv \frac{(1+14d+d^2)^3}{d(1-d)^4} \pmod{p}, \tag{2.1}$$

where $x, d \in \mathbb{F}_p \setminus \{0,1\}$, $d \not\equiv -1 \pmod{p}$ and $\left(\frac{d}{p}\right)_L = -1$. Let

$$W(x) = (x^2+14x+1)^3 d(1-d)^4 - (d^2+14d+1)^3 x(1-x)^4 \equiv 0 \pmod{p}. \tag{2.2}$$

It is trivial that for $x = d$ and $x = d^{-1}$ we have $W(x) \equiv 0 \pmod{p}$. Therefore the polynomial $W(x)$ can be written as

$$W(x) = (x-d)(x-d^{-1})(Ax^4+Bx^3+Cx^2+Dx+E) \equiv 0 \pmod{p}. \tag{2.3}$$

Comparing the coefficients of (2.2) and (2.3), we obtain

$$\begin{aligned} A &= E = d(d-1)^4 \\ B &= D = -4d(d^4+188d^3+646d^2+188d+1) \\ C &= 6d^5 - 2584d^4 + 13348d^3 - 2584d^2 + 6d \end{aligned}$$

Notice that $A \neq 0$, so let's consider

$$F(x) = x^4 + B'x^3 + C'x^2 + B'x + 1, \tag{2.4}$$

where $B' = \frac{B}{A}, C' = \frac{C}{A}$. It remains to prove that the congruence

$$F(x) \equiv 0 \pmod{p}$$

has no solutions in $\mathbb{F}_p$. Consider the substitution

$$a = C' - \frac{3B'^2}{8}, \quad b = B' - \frac{B'C'}{2} + \frac{B'^3}{8} \quad c = 1 - \frac{B'^2}{4} + \frac{B'^2C'}{16} + \frac{3B'^4}{256} \tag{2.5}$$

and $y = x + \frac{B'}{4}$. We have

$$F(x) = y^4 + ay^2 + by + c,$$

so it is enough to consider the following congruence

$$G(y) = y^4 + ay^2 + by + c \equiv 0 \pmod{p}. \tag{2.6}$$

Let us define

$$\Delta_{a,b,c} = -(4a^3+27b^2)b^2 + 16c(a^4 - 8a^2c + 9ab^2 + 16c^2). \tag{2.7}$$

For $F(x)$ we have

$$\Delta_{a,b,c} = \frac{-2^{44}(d^2-34d+1)^2(d+1)^4(d^2+14d+1)^4 d^3}{(d-1)^{22}}. \tag{2.8}$$

We will use the following Lemma:

Lemma 2.2. *Let p be an odd prime, $a, b, c \in \mathbb{Z}$ and $p \nmid b\Delta_{a,b,c}$. If there is an integer $z \in \mathbb{Z}$ such that $z^3 + 2az^2 + (a^2-4c)z - b^2 \equiv 0 \pmod{p}$ and $\left(\frac{z}{p}\right)_L = -1$, then the congruence $y^4 + ay^2 + by + c \equiv 0 \pmod{p}$ is unsolvable.*

Proof of Lemma 2.2. It follows from [5, Lemma 5.2]. ⊠

For the congruence (2.6)

$$b\Delta_{a,b,c} = \frac{2^{57}(d^2-34d+1)^2(d+1)^6(d^2+14d+1)^6(d^4+188d^3+646d^2+188d+1)d^4}{(d-1)^{34}}.$$

It is easy to show that $d^2-34d+1 \equiv 0 \pmod{p}$ has no solutions $p \equiv 3 \pmod{8}$, because 288 is not a quadratic residue modulo p. We still need to show that the congruence $d^4+188d^3+646d^2+188d+1 \equiv 0 \pmod{p}$ has no solutions for $p \equiv 3 \pmod{8}$. Proceeding as above, for this congruence we have that $p \nmid b\Delta_{a,b,c} = 2^{58}\cdot 17 \cdot 47$ and there exists $z \equiv 8192 \pmod{p}$, so from Lemma 2.2 this congruence is unsolvable. Then for (2.6) we have that

$$b\Delta_{a,b,c} \not\equiv 0 \pmod{p} \iff p \nmid b\Delta_{a,b,c}.$$

For

$$z \equiv 2^{12}\cdot\frac{d(d+1)^2(d^2+14d+1)^2}{(d-1)^8} \pmod{p} \tag{2.9}$$

we see that $z^3+2az^2+(a^2-4c)z-b^2 \equiv 0 \pmod{p}$ and

$$\begin{aligned}\left(\frac{z}{p}\right)_L &= \left(\frac{2^{12}}{p}\right)_L\left(\frac{d}{p}\right)_L\left(\frac{(d+1)^2}{p}\right)_L\left(\frac{(d^2+14d+1)^2}{p}\right)_L\left(\frac{(d-1)^{-8}}{p}\right)_L\\ &= \left(\frac{d}{p}\right)_L = -1,\end{aligned}$$

therefore the congruence (2.6) has no solutions by Lemma 2.2 and $x = d$ i $x = d^{-1}$ are the only solutions of the congruence (2.1).

(b) Let d be a quadratic residue modulo p. We need to show that the congruence (2.6) has two distinct solutions. We will need a following Lemma:

Lemma 2.3. *Let $p > 3$ be a prime, $a, b, c \in \mathbb{Z}$ and $p \nmid bD(a,b,c)$. Then congruence*

$$y^4+ay^2+by+c \equiv 0 \pmod{p} \tag{*}$$

has exactly two solutions if and only if congruence

$$z^3+2az^2+(a^2-4c)z-b^2 \equiv 0 \pmod{p} \tag{**}$$

has one and only one solution and the unique solution of $(**)$ is a quadratic residue modulo p. Furthermore, if $z \equiv u^2 \pmod{p}$ is the unique solution of $(**)$ and

$$v^2 \equiv -u^4-2au^2-2bu \pmod{p},$$

the the two solutions of $(*)$ are given by

$$y \equiv \frac{1}{2}\left(u \pm \frac{v}{u}\right).$$

Proof. It follows from [5, Theorem 5.4]. ⊠

For the polynomial $x^3+a_1x^2+a_2x+a_3 = (x-x_1)(x-x_2)(x-x_3)$ we define its discriminant by

$$D = (x_1-x_2)^2(x_1-x_3)^2(x_2-x_3)^2 = a_1^2a_2^2-4a_2^3-4a_1^3a_3-27a_3^2+18a_1a_2a_3. \tag{2.10}$$

Lemma 2.4. *The congruence $x^3+a_1x^2+a_2x+a_3 \equiv 0 \pmod{p}$, where $p \nmid D$*

- *is unsolvable or has 3 solutions, if $\left(\frac{D}{p}\right)_L = 1$;*

- *has 1 solution, if* $\left(\frac{D}{p}\right)_L = -1$.

Proof. It follows from [1, p. 198–199]. ☒

Let us again consider

$$f(z) = z^3 + 2az^2 + (a^2 - 4c)z - b^2 \equiv 0 \pmod{p}.$$

The discriminant of $f(z)$ is equal to

$$D = -\frac{2^{44} \cdot (d+1)^4 \cdot (d^2 + 14d + 1)^4 \cdot d^3 \cdot \left(d^2 - 34d + 1\right)^2}{(d-1)^{22}}.$$

We have that $D \not\equiv 0 \pmod{p}$ and

$$\left(\frac{D}{p}\right)_L = -\left(\frac{d}{p}\right)_L = -1.$$

We take the same z given by (2.9), for which now

$$\left(\frac{z}{p}\right)_L = \left(\frac{d}{p}\right)_L = 1.$$

The congruence (2.6) then has two distinct solutions, so the congruence (2.1) has four distinct solutions. From (2.3), (2.4), (2.5) and Lemma 2.3 we have that those two solutions are given by

$$x \equiv \frac{1}{2}\left(u \pm \frac{v}{u}\right) - \frac{B'}{4A} \pmod{p}, \tag{2.11}$$

where $u^2 = z = (2^{12}d(1+d)^2(1+14d+d^2)^2)/(d-1)^8$. One can then verify that

$$x_1 \equiv \left(\frac{d^{\frac{1}{4}} + 1}{d^{\frac{1}{4}} - 1}\right)^4 \pmod{p}, \tag{2.12}$$

$$x_2 \equiv \left(\frac{d^{\frac{1}{4}} - 1}{d^{\frac{1}{4}} + 1}\right)^4 \pmod{p}. \tag{2.13}$$

Clearly, x_1 and x_2 are both quadratic residues modulo p.

(c) Notice that

$$\frac{16(1+14d+d^2)^3}{d(1-d)^4} \equiv 1728 \pmod{p}$$

can be written as

$$(d+1)^2(d^2 - 34d + 1)^2 \equiv 0 \pmod{p}.$$

for $p \equiv 3 \pmod{8}$ the congruence $d^2 - 34d + 1 \equiv 0 \pmod{p}$ has no solutions as 288 is a quadratic nonresidue modulo p. We obtain one unique solution $d \equiv -1 \pmod{p}$. ☒

Proof of Theorem 1.1 for $p \equiv 3 \pmod{8}$. We can now proceed to calculate the sum (1.3) for $p \equiv 3 \pmod{8}$. From Lemma 2.1 we have that

$$\mathcal{S}_p \equiv 4 \sum_{\substack{d \neq 1 \\ QR}} \frac{(1+14d+d^2)^3}{d(1-d)^4} + 8\left(\sum_{\substack{d \\ QNR}} \frac{(1+14d+d^2)^3}{d(1-d)^4}\right) + \frac{1728}{2} \pmod{p}. \tag{2.14}$$

Lets first consider the sum

$$\sum_{k=2}^{p-1} \frac{(1+14k+k^2)^3}{k(k-1)^4}. \tag{2.15}$$

Notice that

$$\sum_{k=2}^{p-1} \frac{(1+14k+k^2)^3}{k(k-1)^4} = \sum_{\substack{d\neq 1\\ QR}} \frac{(1+14d+d^2)^3}{d(1-d)^4} + \sum_{\substack{d\\ QNR}} \frac{(1+14d+d^2)^3}{d(1-d)^4}. \tag{2.16}$$

By partial fraction decomposition we have

$$\sum_{k=2}^{p-1} \frac{(1+14k+k^2)^3}{k(k-1)^4} = \sum_{k=2}^{p-1} \left(46 + \frac{4096}{(k-1)^4} + \frac{8192}{(k-1)^3} + \frac{4864}{(k-1)^2} + \frac{768}{(k-1)} + \frac{1}{k} + k\right).$$

We will use well know formulas for power sums and the fact that there exist a trivial bijection $\mathbb{Z}_p \to \mathbb{Z}_p$ such that $x \to x^{-1}$. Let

$$\begin{aligned}
s_1 &= \sum_{k=2}^{p-1} 1 \equiv -2 \pmod p\\
s_2 &= \sum_{k=2}^{p-1} \frac{1}{(k-1)^4} \equiv \sum_{k=1}^{p-2} \frac{1}{k^4} \equiv \sum_{k=1}^{p-1} \frac{1}{k^4} - \frac{1}{(p-1)^4} \equiv -1 \pmod p\\
s_3 &= \sum_{k=2}^{p-1} \frac{1}{(k-1)^3} \equiv \sum_{k=1}^{p-2} \frac{1}{k^3} \equiv \sum_{k=1}^{p-1} \frac{1}{k^3} - \frac{1}{(p-1)^3} \equiv 1 \pmod p\\
s_4 &= \sum_{k=2}^{p-1} \frac{1}{(k-1)^2} \equiv \sum_{k=1}^{p-2} \frac{1}{k^2} \equiv \sum_{k=1}^{p-1} \frac{1}{k^2} - \frac{1}{(p-1)^2} \equiv -1 \pmod p\\
s_5 &= \sum_{k=2}^{p-1} \frac{1}{k-1} \equiv \sum_{k=1}^{p-2} \frac{1}{k} \equiv \sum_{k=1}^{p-1} \frac{1}{k} - \frac{1}{p-1} \equiv 1 \pmod p\\
s_6 &= \sum_{k=2}^{p-1} \frac{1}{k} \equiv \sum_{k=1}^{p-1} \frac{1}{k} - 1 \equiv -1 \pmod p\\
s_7 &= \sum_{k=2}^{p-1} k \equiv \sum_{k=1}^{p-1} k - 1 \equiv -1 \pmod p.
\end{aligned}$$

Therefore we obtain that

$$\sum_{k=2}^{p-1} \frac{(1+14k+k^2)^3}{k(k-1)^4} \equiv -2\cdot 46 - 4096 + 8192 - 4864 + 768 - 1 - 1 \equiv -94 \pmod p. \tag{2.17}$$

Notice that

$$\sum_{\substack{d\neq 1\\ QR}} \frac{(1+14d+d^2)^3}{d(1-d)^4} = \frac{1}{2}\sum_{k=2}^{p-2} \frac{(1+14k^2+k^4)^3}{k^2(k^2-1)^4}.$$

Proceeding as before, we have

$$\sum_{k=2}^{p-2}\frac{(1+14k^2+k^4)^3}{k^2(k^2-1)^4}=\sum_{k=2}^{p-2}\Bigg(46+\frac{256}{(k-1)^4}+\frac{512}{(k-1)^3}+\frac{320}{(k-1)^2}+\frac{64}{(k-1)}+\frac{1}{k^2}$$
$$+k^2+\frac{256}{(k+1)^4}-\frac{512}{(k+1)^3}+\frac{320}{(k+1)^2}-\frac{64}{(k+1)}\Bigg).$$

Using results for (2.15), we calculate

$$s_1'=\sum_{k=2}^{p-2}1\equiv-3 \pmod p$$
$$s_2'=\sum_{k=2}^{p-2}\frac{1}{(k-1)^4}\equiv-1-16^{-1} \pmod p$$
$$s_3'=\sum_{k=2}^{p-2}\frac{1}{(k-1)^3}\equiv1+8^{-1} \pmod p$$
$$s_4'=\sum_{k=2}^{p-2}\frac{1}{(k-1)^2}\equiv-1-4^{-1} \pmod p$$
$$s_5'=\sum_{k=2}^{p-2}\frac{1}{k-1}\equiv1+2^{-1} \pmod p$$
$$s_6'=\sum_{k=2}^{p-2}\frac{1}{k^2}\equiv-2 \pmod p$$
$$s_7'=\sum_{k=2}^{p-2}k^2\equiv-2 \pmod p$$
$$s_8'=\sum_{k=2}^{p-2}\frac{1}{(k+1)^4}\equiv-1-16^{-1} \pmod p$$
$$s_9'=\sum_{k=2}^{p-2}\frac{1}{(k+1)^3}\equiv-1-8^{-1} \pmod p$$
$$s_{10}'=\sum_{k=2}^{p-2}\frac{1}{(k+1)^2}\equiv-1-4^{-1} \pmod p$$
$$s_{11}'=\sum_{k=2}^{p-2}\frac{1}{k+1}\equiv-1-2^{-1} \pmod p$$

.

We have that

$$\begin{aligned}\sum_{k=2}^{p-2} \frac{(1+14k^2+k^4)^3}{k^2(k^2-1)^4} &\equiv 46 \cdot (-3) + 256 \cdot \left(-1-16^{-1}\right) + 512 \cdot \left(1+8^{-1}\right) \\ &+ 320 \cdot \left(-1-4^{-1}\right) + 64 \cdot \left(1+2^{-1}\right) - 2 - 2 \\ &+ 256 \cdot \left(-1-16^{-1}\right) - 512 \cdot \left(-1-8^{-1}\right) + 320 \cdot \left(-1-4^{-1}\right) \\ &- 64 \cdot \left(-1-2^{-1}\right) \equiv -142 \pmod{p}.\end{aligned}$$

Therefore

$$\sum_{\substack{d \neq 1 \\ QR}} \frac{(1+14d+d^2)^3}{d(1-d)^4} \equiv -71 \pmod{p}. \tag{2.18}$$

From (2.16) we have that

$$\sum_{\substack{d \\ QNR}} \frac{(1+14d+d^2)^3}{d(1-d)^4} \equiv -23 \pmod{p}. \tag{2.19}$$

Going back to (2.14):

$$S_p \equiv 4 \cdot (-71) + 8 \cdot (-23) + \frac{1728}{2} \equiv 396 \pmod{p}. \tag{2.20}$$

⊠

3. Case $p \equiv 7 \pmod 8$

As in the previous case, we will first prove the following Lemma:

Lemma 3.1. *If for* $p \equiv 7 \pmod 8$ *the congruence*

$$\frac{16(1+14d+d^2)^3}{d(1-d)^4} \equiv j_0 \pmod{p},$$

where $j_0 \not\equiv 0 \pmod p$ *has a solution, then one of the following three cases occurs:*

- *(a) Two distinct elements* d_0, d_0^{-1} *are solutions, neither of which is a quadratic residue modulo p. The set of quadratic nonresidues is denoted as QNR.*
- *(b) Four distinct elements* $d_1, d_1^{-1}, d_2, d_2^{-1}$ *are solutions, and all of them are quadratic residues modulo p. The set of quadratic residues is denoted as QR.*
- *(c) If the element* $d_3 = p - 1$ *is a solution, then there exist two additional distinct solutions* d_4, d_4^{-1} *that are quadratic residues modulo p.*

Proof of Lemma 3.1. (a) Notice that if $p \equiv 3, 7 \pmod 8$, then $p \equiv 3 \pmod 4$, therefore the proof is identical to the part a) of proof for Lemma 2.1.

(b) Follows from part b) of proof for Lemma 2.1.

(c) Similar to part c) of proof for Lemma 2.1 we have that

$$(d+1)^2(d^2-34d+1)^2 \equiv 0 \pmod{p}.$$

For $p \equiv 7 \pmod 8$ the congruence $d^2 - 34d + 1 \equiv 0 \pmod p$ has two solutions, since 288 is a quadratic residue modulo p and for $p \equiv 7 \pmod 8$ 2 is also a quadratic residue. Both solutions then are quadratic residues modulo p, precisely

$$d \equiv 17 \pm 12a \pmod p,$$

whre $a \in \mathbb{F}_p$ such that $a^2 = 2$. Then

$$d \equiv (3 \pm 2a)^2 \equiv (1 \pm a)^4 \pmod p.$$

⊠

Proof of Theorem 1.1 for $p \equiv 7 \pmod p$. Let us calculate the sum S_p for $p \equiv 7 \pmod p$. From Lemma 3.1 we have that

$$\mathcal{S}_p = 4 \sum_{\substack{d \neq 1 \\ QR}} \frac{16(1+14d+d^2)^3}{d(1-d)^4} + 8 \sum_{\substack{d \\ QNR}} \frac{(1+14d+d^2)^3}{d(1-d)^4}. \tag{3.1}$$

Using (2.18) and (2.19), we obtain

$$\mathcal{S}_p \equiv 4 \cdot (-71) + 8 \cdot (-23) \equiv -468 \pmod p.$$

⊠

4. Case $p \equiv 5 \pmod 8$

Lemma 4.1. *If for $p \equiv 5 \pmod 8$ the congruence*

$$\frac{16(1+14d+d^2)^3}{d(1-d)^4} \equiv j_0 \pmod p,$$

where $j_0 \not\equiv 0 \pmod p$ has a solution, then one of the following three cases occurs:

(a) Two distinct elements d_0, d_0^{-1} are solutions, neither of which is a quadratic residue modulo p. The set of quadratic nonresidues is denoted as QNR.

(b) Six distinct elements $d_1, d_1^{-1}, d_2, d_2^{-1}, d_3, d_3^{-1}$, which are all quadratic residues modulo p are solutions, if for all of them the congruence

$$x^4 \equiv d' \pmod p, \quad d' \in \{d_1, d_1^{-1}, d_2, d_2^{-1}, d_3, d_3^{-1}\}$$

is solvable. We call such elements biquadratic residues modulo p. The set of biquadratic residues modulo p is denoted as BQR.

(c) Two distinct elements d_4, d_4^{-1}, which are quadratic residues modulo p are solutions, if for all of them the congruence

$$x^4 \equiv d' \pmod p, \quad d' \in \{d_4, d_1^{-1}\}$$

is not solvable. The set of elements that are quadratic residues, but are not biquadratic residues modulo p is denoted as a difference of sets $QR \setminus BQR$.

(d) The element $d = p - 1$ is the only solution for which $j_0 \equiv 1728 \pmod p$.

Proof of Lemma 4.1. a) Follows from part a) of proof for Lemma 2.1.

b, c) Assume that the congruence (2.3) has 6 solutions and all of them are quadratic residue modulo p. Then the congruence (2.6) has 4 such solutions. Consider the following Lemma:

Lemma 4.2. *Let $p > 3$ be prime, $a, b, c \in \mathbb{Z}$ and $p \nmid bD(a, b, c)$. Then congruence $(*)$ $x^4 + ax^2 + bx + c \equiv 0 \pmod{p}$ has four solutions if and only if congruence $(**)$ $y^3 + 2ay^2 + (a^2 - 4c)y - b^2 \equiv 0 \pmod{p}$ has three solutions and all the three solutions are quadratic residues modulo p. Furthermore, if $y \equiv u_1^2, u_2^2, u_3^2 \pmod{p}$ $(u_1, u_2, u_3 \in Z)$ are the solutions of $(**)$ such that $u_1u_2u_3 \equiv -b \pmod{p}$, then the four solutions of $(*)$ are given by*

$$x \equiv \frac{u_1 + u_2 + u_3}{2}, \frac{u_1 - u_2 - u_3}{2}, \frac{-u_1 + u_2 - u_3}{2}, \frac{-u_1 - u_2 + u_3}{2} \pmod{p}.$$

Proof. Follows from [5, Theorem 5.6]. ☒

Consider the congruence

$$y^3 + 2ay^2 + (a^2 - 4c)y - b^2 \equiv 0 \pmod{p},$$

where a, b are given by (2.5). It has 3 solutions, namely:

$$y_1 \equiv 2^{12}d\left(\frac{(d+1)(d^2+14d+1)}{(d-1)^4}\right)^2 \pmod{p}$$

$$y_2 \equiv \frac{\begin{array}{l}128(22d^7 + 1052d^6 + 7882d^5 + 14856d^4 + \\ \quad 7882d^3 + 1052d^2 + \sqrt{-d\left(d^2-34d+1\right)^2\left(d-1\right)^{10}} + 22d)\end{array}}{\left(d-1\right)^8} \pmod{p}$$

$$y_3 \equiv \frac{\begin{array}{l}128(22d^7 + 1052d^6 + 7882d^5 + 14856d^4 + \\ \quad 7882d^3 + 1052d^2 - \sqrt{-d\left(d^2-34d+1\right)^2\left(d-1\right)^{10}} + 22d)\end{array}}{\left(d-1\right)^8} \pmod{p}.$$

It is obvious that y_1 is a quadratic residue modulo p. In our case $p \equiv 1 \pmod{4}$, so -1 is a quadratic residue modulo p. Let us write $d = m^2$ and $i^2 = -1$, $m, d \in \mathbb{Z}$. We have that

$$y_2 \equiv \frac{128im(m+i)^2(m^2+i4m-1)^2(m^4-16im^3-34m^2+i16m+1)^2}{(m^2-1)^8} \pmod{p}$$

$$y_3 \equiv \frac{-128im(m-i)^2(m^2-4im-1)^2(m^4+i16m^3-34m^2-16im+1)^2}{(m^2-1)^8} \pmod{p}.$$

Notice that

$$\left(\frac{y_2}{p}\right)_L = \left(\frac{y_3}{p}\right)_L = \left(\frac{2}{p}\right)_L \left(\frac{m}{p}\right)_L \left(\frac{i}{p}\right)_L = -\left(\frac{m}{p}\right)_L \left(\frac{i}{p}\right)_L,$$

since 2 is a quadratic nonresidue modulo $p \equiv 5 \pmod{8}$. Gauss in his work [2] proved that

$$\left(\frac{i}{p}\right)_L = 1 \iff p \equiv 1 \pmod{8},$$

therefore we have that

$$\left(\frac{y_2}{p}\right)_L = \left(\frac{y_3}{p}\right)_L = \left(\frac{m}{p}\right)_L.$$

Both solutions y_2 and y_3 are then quadratic residues modulo p, if m is a quadratic residue. We can then write $m = k^2$, $k \in \mathbb{Z}$, so $d = k^4$. Using Lemma 4.2 we verify that

$$\sqrt{y_1y_2y_3} \equiv -b \pmod{p}$$

and the four solutions to (2.4) are

$$x_1 \equiv \left(\frac{d^{\frac{1}{4}}+1}{d^{\frac{1}{4}}-1}\right)^4 \pmod{p}, \tag{4.1}$$

$$x_2 \equiv \left(\frac{d^{\frac{1}{4}}-1}{d^{\frac{1}{4}}+1}\right)^4 \pmod{p}, \tag{4.2}$$

$$x_3 \equiv \left(\frac{d^{\frac{1}{4}}-i}{d^{\frac{1}{4}}+i}\right)^4 \pmod{p}, \tag{4.3}$$

$$x_4 \equiv \left(\frac{d^{\frac{1}{4}}+i}{d^{\frac{1}{4}}-i}\right)^4 \pmod{p}. \tag{4.4}$$

It is clear that every solution is a biquadratic residue modulo p. If m is a quadratic nonresidue, then $d^{\frac{1}{4}}$ does not exist in $\mathbb{Z}_p$ and from Lemma 2.2 the congruence (2.6) is unsolvable. Then there are two solutions of (2.3), which are quadratic residues modulo p.

(d) Follows from part c) of proof for Lemma 4.1. ☒

Proof of Theorem 1.1 for $p \equiv 5 \pmod{p}$. Notice that is the set $\{2,\dots,p-1\}$ there are exactly $\frac{p-5}{4}$ biquadratic residues modulo p. Consider

$$\sum_{\substack{k\neq 1\\ BQR}} \frac{(1+14k+k^2)^3}{k(k-1)^4} = \sum_{\substack{k\neq 1\\ BQR}} \left(46 + \frac{4096}{(k-1)^4} + \frac{8192}{(k-1)^3} + \frac{4864}{(k-1)^2} + \frac{768}{(k-1)} + \frac{1}{k} + k\right).$$

We calculate the sums individually

$$s''_1 = \sum_{\substack{k\neq 1\\ BQR}} 1 = \frac{p-5}{4} \equiv -2^{-2}\cdot 5 \pmod{p}$$

$$s''_2 = \sum_{\substack{k\neq 1\\ BQR}} \frac{1}{(k-1)^4} \equiv -2^{-12}\cdot 1979 \pmod{p}$$

$$s''_3 = \sum_{\substack{k\neq 1\\ BQR}} \frac{1}{(k-1)^3} \equiv 2^{-7}\cdot 65 \pmod{p}$$

$$s''_4 = \sum_{\substack{k\neq 1\\ BQR}} \frac{1}{(k-1)^2} \equiv -2^{-6}\cdot 35 \pmod{p}$$

$$s''_5 = \sum_{\substack{k\neq 1\\ BQR}} \frac{1}{k-1} \equiv 2^{-3}\cdot 5 \pmod{p}$$

$$s''_6 = \sum_{\substack{k\neq 1\\ BQR}} \frac{1}{k} \equiv \frac{1}{4}\sum_{k=1}^{p-1}\frac{1}{k^4} - 1 \equiv -1 \pmod{p}$$

$$s_7'' = \sum_{\substack{k\neq 1\\ BQR}} k \equiv \frac{1}{4}\sum_{k=1}^{p-1} k^4 - 1 \equiv -1 \pmod{p},$$

therefore

$$\begin{aligned}\sum_{\substack{k\neq 1\\ BQR}} \frac{(1+14k+k^2)^3}{k(k-1)^4} &\equiv 46\left(-5\cdot 2^{-1}\right) + 4096\left(-1979\cdot 2^{-12}\right) + 8192\left(65\cdot 2^{-7}\right)\\ &\quad + 4864\left(-35\cdot 2^{-6}\right) + 768\left(5\cdot 2^{-3}\right) - 1 - 1\\ &\equiv -117\cdot 2^{-1} \pmod{p}. \end{aligned}\tag{4.5}$$

Using the result from (2.18), we obtain

$$\sum_{\substack{k\neq 1\\ QR}} \frac{(1+14k+k^2)^3}{k(k-1)^4} = \sum_{\substack{k\neq 1\\ BQR}} \frac{(1+14k+k^2)^3}{k(k-1)^4} + \sum_{\substack{k\neq 1\\ QR\backslash BQR}} \frac{(1+14k+k^2)^3}{k(k-1)^4} \equiv -71 \pmod{p},\tag{4.6}$$

so

$$\sum_{\substack{k\neq 1\\ QR\backslash BQR}} \frac{(1+14k+k^2)^3}{k(k-1)^4} \equiv -25\cdot 2^{-1} \pmod{p}.\tag{4.7}$$

From Lemma 4.1 we have that

$$\mathcal{S}_p = 8\sum_{\substack{k\\ QNR}} \frac{(1+14k+k^2)^3}{k(k-1)^4} + \frac{8}{3}\sum_{\substack{k\neq 1\\ BQR}} \frac{(1+14k+k^2)^3}{k(k-1)^4} + 8\sum_{\substack{k\neq 1\\ QR}} \frac{(1+14k+k^2)^3}{k(k-1)^4} + \frac{1728}{2}.$$

From (2.19), (4.5) and (4.7) we finally get that

$$\mathcal{S}_p \equiv 8(-23) + \frac{8}{3}\left(\frac{-117}{2}\right) + 8\left(\frac{-25}{2}\right) + \frac{1728}{2} \equiv 424 \pmod{p}.$$

$\boxtimes$

5. Case $p \equiv 1 \pmod 8$

Lemma 5.1. *If for* $p \equiv 1 \pmod 8$ *the congruence*

$$\frac{16(1+14d+d^2)^3}{d(1-d)^4} \equiv j_0 \pmod{p},$$

where $j_0 \not\equiv 0 \pmod{p}$ *has a solution, then one of the following three cases occurs:*

(a) Two distinct elements d_0, d_0^{-1} *are solutions, neither of which is a quadratic residue modulo* p*. The set of quadratic nonresidues is denoted as* QNR*.*

(b) Six distinct elements $d_1, d_1^{-1}, d_2, d_2^{-1}, d_3, d_3^{-1}$*, which are all quadratic residues modulo* p *are solutions, if for all of them the congruence*

$$x^4 \equiv d' \pmod{p}, \quad d' \in \{d_1, d_1^{-1}, d_2, d_2^{-1}, d_3, d_3^{-1}\}$$

is solvable. We call such elements biquadratic residues modulo p*. The set of biquadratic residues modulo* p *is denoted as* BQR*.*

(c) Two distinct elements d_4, d_4^{-1}, which are quadratic residues modulo p are solutions, if for all of them the congruence

$$x^4 \equiv d' \pmod{p}, \quad d' \in \{d_4, d_1^{-1}\}$$

is not solvable. The set of elements that are quadratic residues, but are not biquadratic residues modulo p is denoted as a difference of sets $QR \setminus BQR$.

(d) If the element $d = p-1$ is a solution, then there exist additional two distinct solutions d_6, d_6^{-1} which are biquadratic residues modulo p.

Proof. $a)$ Follows from part $a)$ of proof for Lemma 3.1.

$b, c)$ Similarly as in parts $b, c)$ of proof for Lemma 4.1, we now have

$$\left(\frac{y_2}{p}\right)_L = \left(\frac{y_3}{p}\right)_L = \left(\frac{2}{p}\right)_L \left(\frac{m}{p}\right)_L \left(\frac{i}{p}\right)_L = \left(\frac{m}{p}\right)_L \left(\frac{i}{p}\right)_L,$$

since 2 is a quadratic residue modulo p and

$$\left(\frac{i}{p}\right)_L = 1.$$

In order for y_2, y_3 to be quadratic residues modulo p, m must again be a quadratic residue modulo p and we come to the same conclusion as in parts $b, c)$ of proof for Lemma 4.1.

$d)$ Follows from part $c)$ of proof for Lemma 3.1.

⊠

Proof of 1.1 for $p \equiv 1 \pmod{8}$. Notice that the sum S_p is the same as in case when $p \equiv 5 \pmod{8}$. Now $j-$invariant is being generated by the element $p-1$, which is a biquadratic residue modulo p and also by two different biquadratic residues, therefore instead of six solutions we obtain three and again we need to add $\frac{1728}{2}$ at the end to get a single $j-$invariant 1728.

$$\mathcal{S}_p \equiv 8(-23) + \frac{8}{3}\left(\frac{-117}{2}\right) + 8\left(\frac{-25}{2}\right) + \frac{1728}{2} \equiv 424 \pmod{p}.$$

⊠

References

[1] H. Cohen. *A Course in Computational Algebraic Number Theory*. Springer, Berlin, 1993.

[2] Carl Friedrich Gauss and Arthur A. Clarke. *Disquisitiones Arithmeticae*. Yale University Press, 1965.

[3] Jędrzej Miarecki. *Elliptic Curves*. Bachelor's thesis, University of Wrocław, Wrocław, Poland, 2024. Originally written in Polish. Polish title: Krzywe eliptyczne.

[4] J.-P. Serre. *A course in arithmetic*. Graduate Texts in Mathematics, No. 7. Springer-Verlag, New York-Heidelberg, 1973. Translated from the French.

[5] Zhi-Hong Sun. Cubic and quartic congruences modulo a prime. *Journal of Number Theory*, 102:41–89, 2003.