Contemporary Mathematics

On pairs of primes with small order reciprocity

Craig Costello and Gaurish Korpal

Abstract. We give a sieving algorithm for finding pairs of primes with small multiplicative orders modulo each other. This problem is a necessary condition for obtaining constructions of 2-cycles of pairing-friendly curves, which have found use in cryptographic applications. Our database of examples suggests that, except for a well-known infinite family of such primes, instances become increasingly rare as the size of the primes increase. This leads to some interesting open questions for which we hope our database prompts further investigation.

1. The problem

This paper is concerned with finding pairs of primes that satisfy certain instances of the following definition.

Definition 1.1 (Primes with (k, k')-order reciprocity). The prime numbers p and q have (k, k')-*order reciprocity* if $\mathrm{ord}_q(p) = k$ and $\mathrm{ord}_p(q) = k'$. That is, k and k' are the smallest natural numbers such that $p^k \equiv 1 \pmod{q}$ and $q^{k'} \equiv 1 \pmod{p}$.

Herein we are interested in instances of Definition 1.1 where p and q are *large* and where k and k' are *small*. To be more concrete about what we mean by large and small, we must first discuss why this problem finds practical relevance in cryptography. In 2014, Ben-Sasson, Chiesa, Tromer, and Virza [**BSCTV14**] showed that certain types of pairing-based zero-knowledge proof systems can be instantiated in a very efficient and scalable way if we have a 2-*cycle* of *pairing-friendly* elliptic curves. Let p and q be large primes. We say that the elliptic curves $E/\mathbb{F}_p$ and $E'/\mathbb{F}_q$ are a 2-cycle if and only if $\#E(\mathbb{F}_p) = q$ and $\#E'(\mathbb{F}_q) = p$. Furthermore, we say that $E/\mathbb{F}_p$ is pairing-friendly if its *embedding degree* $k = \mathrm{ord}_q(p)$ is small enough for the order-q Weil and/or Tate pairings to be efficiently computable. Similarly, we say that $E'/\mathbb{F}_q$ is pairing-friendly p if its embedding degree $k' = \mathrm{ord}_p(q)$ is suitably small. These embedding degrees need to be small enough that the pairings in $\mathbb{F}_{p^k}^{\times}$ and $\mathbb{F}_{q^{k'}}^{\times}$ can be computed efficiently. In practice, and indeed in this paper, we follow the standard rule-of-thumb and impose that both k and k' are no larger than 50 [**FST10**].

2020 *Mathematics Subject Classification.* Primary 11A07, 11T22, 11T71, 11A15, 11Y16.
Part of this work was done while Gaurish was an intern at Microsoft Research.

On the other hand, for the associated proof system to be cryptographically secure, the elliptic curve discrete logarithm problems (ECDLPs) and the finite field discrete logarithm problems (DLPs) all need to be computationally infeasible. In practice, this means p and q must both be at least 2^{160} for ECDLP security, and k and k' must be large enough for the fields $\mathbb{F}_{p^k}$ and $\mathbb{F}_{q^{k'}}$ to offer comparable DLP security.

1.1. A necessary condition for 2-cycles. The only known instances of 2-cycles of ordinary pairing-friendly elliptic curves arise from the Miyaji-Nakabayashi-Takano (MNT) family [**MNT01**], which is parameterised as

$$p = x^2 - x + 1 \qquad \text{and} \qquad q = x^2 + 1, \tag{1.1}$$

from which it follows that $(k, k') = (\mathrm{ord}_q(p), \mathrm{ord}_p(q))$ are always such that $k \mid 6$ and $k' \mid 4$.

It turns out that the MNT 2-cycle is suboptimal in practical applications, because the embedding degrees are too small to optimally balance the ECDLP and DLP securities. With $(k, k') = (4, 6)$, meeting the requisite DLP security requires that $\mathbb{F}_{p^4}$ and $\mathbb{F}_{q^6}$ are at least a few thousand bits [**SG18**, Table 1], which forces the sizes of p and q to be orders of magnitude larger than they would be in the optimal scenario where k and k' are larger. The subsequent hunt for 2-cycles of ordinary elliptic curves with larger embedding degrees has only produced negative results [**CCW19, BMUS23**]. For example, Chiesa, Chua and Weidner [**CCW19**] proved that 2-cycles of ordinary elliptic curves $E/\mathbb{F}_p$ and $E'/\mathbb{F}_q$ with $(k, k') \in \{(5, 10), (8, 8), (12, 12)\}$ do not exist. In what follows, we use a toy example to motivate the work in this paper by showing the existence of a 2-cycle with $(k, k') = (12, 12)$ under relaxed conditions, in light of recent work in [**CCN24**].

Example 1.2. The prime pair $(p, q) = (620461, 15493)$ is such that $(k, k') = (\mathrm{ord}_q(p), \mathrm{ord}_p(q)) = (12, 12)$. Proposition 3 of [**CCW19**] rules out the existence of a 2-cycle with $q = \#E(\mathbb{F}_p)$ and $p = \#E'(\mathbb{F}_q)$. Indeed, the Hasse bound for $E'/\mathbb{F}_q$ in this instance is $15246 \leq \#E'(\mathbb{F}_q) \leq 15742$, ruling out $p = \#E'$. If we relax the 2-cycle condition to allow cofactors as in [**CCW19**, §7] and to allow extension fields as in [**CCN24**], we might instead seek to find two elliptic curves $E/\mathbb{F}_p$ and $E'/\mathbb{F}_{q^2}$ such that $\#E(\mathbb{F}_p) = hq$ and $\#E'(\mathbb{F}_{q^2}) = h'p$. While such an E does exist (with $h = 40$), there is no multiple of p inside the Hasse interval for $E'/\mathbb{F}_{q^2}$; $h' = 386$ is too small for $h'p$ to be inside the interval, while $h' = 387$ is too large. If, however, we instead consider a genus 2 curve $C/\mathbb{F}_q$, close examination of the possible group orders of its Jacobian (see [**GKS11**, §2.1]) reveals that $h' \in \{374, \ldots, 399\}$ are all plausible cofactors. Indeed, we readily find one such example as $C/\mathbb{F}_q \colon y^2 = x^6 + 6611x^5 + 13858x^4 + 6818x^3 + 5652x^2 + 10423x + 1795$, which is such that $\#\mathcal{J}_C(\mathbb{F}_q) = 383 \cdot p$, forming a 2-cycle with $E/\mathbb{F}_p \colon y^2 = x^3 + 30984x + 426966$, which is such that $\#E(\mathbb{F}_p) = 40 \cdot q$. Both $\mathcal{J}_C$ and E are ordinary and have embedding degree 12.

The above example shows that it is possible to construct ordinary 2-cycles under relaxed conditions, even when their existence has been ruled out in the case where both curves are elliptic curves of prime order, so long as we have primes with (k, k')-order reciprocity[1]. In our view, the existence of large primes with small order

[1]The notion and terminology *order reciprocity* is found in a 2019 post by Lee [**Lee19**].

reciprocity is *the* fundamental and necessary requirement for determining whether relaxed 2-cycles can exist in the interesting cryptographic ranges.

1.2. Open questions. One can show that there are no prime pairs with $(2,2)$-order reciprocity, but infinitely many prime pairs with $(p-1, q-1)$-order reciprocity[2]. However, in between these two extremes there are a number of questions that are of potential relevance to cryptography. For example, we saw above that the pair $(p,q) = (620461, 15493)$ has $(12,12)$-order reciprocity, but this is the only such example we found. We state some open questions that warrant further investigation:

(1) *Is* $(620461, 15493)$ *the only prime pair with* $(12,12)$*-order reciprocity?*
(2) *Are there any fixed values of* (k,k') *with* $\min(k,k) > 4$ *for which there are an infinite number of primes with* (k,k')*-order reciprocity?*
(3) *Are there any fixed values of* (k,k') *with* $\min(k,k) > 2$ *for which there are no pairs of primes with* (k,k')*-order reciprocity?*

Finally, we pose the question of interest that underlies this work:

(4) *Are there* **any** *large pairs of primes with small* (k,k')*-order reciprocity?*

In the search for answers to the above questions, we derived an algorithm for finding primes with (k,k')-order reciprocity – this is presented in Section 2. We used this algorithm to exhaustively search up to the 200 millionth prime for pairs with small order reciprocity – the database of examples we found is summarised in Section 3.

We reiterate that we are not interested in the known examples which come from the MNT parameterisation in (1.1), and that in practice we are therefore interested in examples with, say, $5 \leq k, k' \leq 50$. By *large* primes, we mean cryptographically large, i.e. at least 2^{160}.

2. The algorithms

Let p be a prime number and let $\alpha_p \in \mathbb{F}_p$ be such that $\mathbb{F}_p^\times = \langle \alpha_p \rangle$, where elements in $\mathbb{F}_p^\times$ are represented by the corresponding least positive remainder in $(\mathbb{Z}/p\mathbb{Z})^\times$. Then Algorithm 1 returns all $q < p$ such that $\mathrm{ord}_q(p) = k$ and $\mathrm{ord}_p(q) = k'$. Furthermore, let P be a list of prime numbers and A be a list such that $A[i]$ is a primitive element modulo $P[i]$. Algorithm 2 finds all the primes pairs (p,q) with $p \in P$ and $q < p$ such that $\mathrm{ord}_q(p) = k$ and $\mathrm{ord}_p(q) = k'$ or $\mathrm{ord}_q(p) = k'$ and $\mathrm{ord}_p(q) = k$.

2.1. Proof of correctness. We start by showing that Algorithm 1 returns all primes $q < p$ such that $\mathrm{ord}_q(p) = k$ and $\mathrm{ord}_p(q) = k'$. Any such q must be the least positive remainder of some power of α_p^t with $t = (p-1)/k'$ in $(\mathbb{Z}/p\mathbb{Z})^\times$; Lines 4-5 exhaust these possibilities, while Line 6 avoids testing those q which cannot have exact order k'. Line 13 only keeps those q which are prime and for which elements of order k exist in $(\mathbb{Z}/q\mathbb{Z})^\times$. The remainder of Algorithm 1 simply keeps those p which have exact order k in $(\mathbb{Z}/q\mathbb{Z})^\times$. Algorithm 2 loops over all combinations of $p, q \in P$ and, for $k \neq k'$, makes an additional call to Algorithm 1 to reverse the order of k and k'.

[2]For the former, $p < q$ implies $p = q - 1$, the only option for which is $(p,q) = (2,3)$, which has $\mathrm{ord}_p(q) = 1$. For the latter, see [**Fre19**].

Algorithm 1 `reciprocity`(p, α_p, k, k')

```
Q ← [] // empty list
if p ≡ 1 (mod k') then
  t ← (p−1)/k'
  for s = 1 to k' − 1 do
    m ← s · t
    if gcd(m, p − 1) = t then
      q ← α_p^m
      if q ≡ 1 (mod k) and q is prime then
        // we have found q such that ord_p(q) = k'.
        if p^k ≡ 1 (mod q) then
          b ← 1
          for d = 1 to k − 1 do
            if k ≡ 0 (mod d) and p^d ≡ 1 (mod q) then
              b ← 0
              break // ord_q(p) ≠ k
          if b = 1 then
            Q.append(q) // ord_q(p) = k
return Q
```

Algorithm 2 `primepairs`(P, A, k, k')

```
L ← [] // empty list
for p in P do
  Q ← reciprocity(p, α_p, k, k')
  if #Q ≠ 0 then
    for q ∈ Q do
      L.append((p, q))
  if k ≠ k' then
    Q' ← reciprocity(p, α_p, k', k)
    if #Q' ≠ 0 then
      for q' ∈ Q' do
        L.append((q', p))
return L
```

2.2. Complexity analysis. Let p be the largest prime in the list P, whose cardinality is N. We will analyse the time complexity of Algorithm 2 as $p \to \infty$, assuming that k and k' remain fixed, small constants. We will also assume that, as $p \to \infty$, the average size of the primes in P is in $O(p)$; this assumption holds if P contains all primes within a given interval and, in particular, if P contains all primes up to p. Algorithm 2 makes either one or two calls to Algorithm 1 for each prime in P, so it follows that the time complexity of Algorithm 2 is in $O(N \cdot R)$, where R is the complexity of Algorithm 1 on input of a prime of size in $O(p)$.

We will now proceed step by step through Algorithm 1, stating the time complexity of each step together with the probability of advancing through the control statements. These can be accumulated in a straightforward way to obtain a precise

big-O complexity of Algorithm 1, but this becomes a rather messy and nonillustrative expression, so we will eventually ignore all logarithmic factors to instead state a final big-$\tilde{O}$ time complexity.

For small, fixed k and k', calls to Algorithm 1 advance to Line 6 $O(p)$ times on average. The time complexity of the GCD algorithm here is in $O(\log p)$ and, heuristically, $O(1)$ of these tests advance to Line 7. The asymptotic complexity of this exponentiation is in $O(\log p \log^2(\log p) \log\log\log p)$, using the Schönhage–Strassen algorithm [**SS71**]. In Line 8, an optimised probabilistic primality test (like Miller-Rabin [**Rab80**]) has time complexity $O(\log^3 p)$, while the deterministic AKS primality test [**AKS04**] has time complexity $O(\log^6 p)$. Since the size of the prime q is in $O(p)$, the probability of advancing to the remaining steps is in $O(1/\log p)$ by the Prime Number Theorem.

It follows that Algorithm 1 has time complexity $\tilde{O}(p)$, and thus that Algorithm 2 has complexity $\tilde{O}(N \cdot p)$. In particular, if P contains all the primes up to p, then Algorithm 2 has complexity $\tilde{O}(p^2)$ by the Prime Number Theorem.

3. The database

We used the `parallel GP` interface of `PARI/GP` [**The24**] running on AMD Ryzen Threadripper PRO 3995WX with 128 GB memory to perform all the computations. The `PARI/GP` implementation of the algorithms and the data are available in

`https://github.com/gkorpal/order-reciprocity`.

Let P_1 be the list of first 100 million primes and P_2 be the list of the next 100 million primes. We first performed the primitive element pre-computation for P_1 and P_2 using the in-built `znprimroot` function [**Coh93**, Algorithm 1.4.4].

We then ran Algorithm 2 to find prime pairs in P_1 and for prime pairs (where the largest prime is) in P_2 with (k, k')-order reciprocity, for $2 \leq k \leq k' \leq 51$. We could not parallelise the outermost for loop of this algorithm because of the memory sharing restrictions. However, we utilized the `parallel GP` interface to simultaneously run the computations for $(k, k') \in \{\{m, m+1\} \times \{n, n+1\} \mid m, n \in 2\mathbb{Z} \text{ and } 2 \leq m \leq n \leq 50\}$ such that $k \leq k'$.

Tables 1 and 2 present sample data, while the repository offers access to the full dataset. Table 1 highlights that $(4, 6)$-order reciprocity remains the most prevalent, even as prime size increases. Meanwhile, Table 2 shows that larger prime sizes result in most (k, k')-order reciprocities yielding no prime pairs.

TABLE 1. Counts of prime pairs with selected (k, k')-order reciprocity. The bottom row counts the number of pairs when the larger prime is in P_2.

(k, k')		$(4, 6)$	$(3, 10)$	$(3, 14)$	$(4, 46)$	$(2, 35)$	$(11, 49)$	$(15, 45)$	$(38, 45)$
#prime	P_1	738	20	14	8	5	4	3	2
pairs	P_2	258	0	0	2	2	3	2	2

TABLE 2. Counts of (k, k')-order reciprocities with selected number of prime pairs. The bottom row counts the number of (k, k')-order reciprocities when the larger prime is in P_2.

#prime pairs		0	1	2	3	4 to 12	14	20	258	738	Total
# (k, k')	P_1	97	147	209	231	588	1	1	0	1	1275
	P_2	1108	159	6	1	0	0	0	1	0	1275

References

[AKS04] M. Agrawal, N. Kayal, and N. Saxena, *PRIMES is in p*, Annals of Mathematics **160** (2004), no. 2, 781–793, Preliminary version appeared in 2002.

[BMUS23] M. Bellés-Muñoz, J. Jiménez Urroz, and J. Silva, *Revisiting cycles of pairing-friendly elliptic curves*, Advances in cryptology—CRYPTO 2023. Part II, LNCS, vol. 14082, Springer, Cham, 2023, pp. 3–37.

[BSCTV14] E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza, *Scalable zero knowledge via cycles of elliptic curves*, Advances in cryptology—CRYPTO 2014. Part II, LNCS, vol. 8617, Springer, Heidelberg, 2014, pp. 276–294.

[CCN24] M. Corte-Real Santos, C. Costello, and M. Naehrig, *On cycles of pairing-friendly abelian varieties*, Advances in cryptology—CRYPTO 2024. Part IX, LNCS, vol. 14928, Springer, Cham, 2024, pp. 221–253.

[CCW19] A. Chiesa, L. Chua, and M. Weidner, *On cycles of pairing-friendly elliptic curves*, SIAM J. Appl. Algebra Geom. **3** (2019), no. 2, 175–192.

[Coh93] H. Cohen, *A course in computational algebraic number theory*, GTM, vol. 138, Springer-Verlag, Berlin, 1993.

[Fre19] FredH, *Order reciprocity*, Mathematics Stack Exchange, 2019, `https://math.stackexchange.com/q/3118669` (version: 2019-02-19).

[FST10] D. Freeman, M. Scott, and E. Teske, *A taxonomy of pairing-friendly elliptic curves*, J. Cryptology **23** (2010), no. 2, 224–280.

[GKS11] P. Gaudry, D. Kohel, and B. Smith, *Counting points on genus 2 curves with real multiplication*, Advances in cryptology—ASIACRYPT 2011, LNCS, vol. 7073, Springer, Heidelberg, 2011, pp. 504–519.

[Lee19] S. Lee, *Order reciprocity*, Mathematics Stack Exchange, 2019, `https://math.stackexchange.com/q/3118453` (version: 2019-02-19).

[MNT01] A. Miyaji, M. Nakabayashi, and S. Takano, *Characterization of elliptic curve traces under FR-reduction*, Information security and cryptology—ICISC 2000, LNCS, vol. 2015, Springer, Berlin, 2001, pp. 90–108.

[Rab80] M. O. Rabin, *Probabilistic algorithm for testing primality*, Journal of Number Theory **12** (1980), no. 1, 128–138.

[SG18] M. Scott and A. Guillevic, *A new family of pairing-friendly elliptic curves*, Arithmetic of finite fields, LNCS, vol. 11321, Springer, Cham, 2018, pp. 43–57.

[SS71] A. Schönhage and V. Strassen, *Schnelle multiplikation großer zahlen*, Computing **7** (1971), no. 3-4, 281–292.

[The24] The PARI Group, Univ. Bordeaux, *PARI/GP version `2.15.5`*, 2024, available from `http://pari.math.u-bordeaux.fr/`.

QUEENSLAND UNIVERSITY OF TECHNOLOGY, BRISBANE, AUSTRALIA
Email address: `craig.costello@qut.edu.au`

UNIVERSITY OF ARIZONA, TUCSON, UNITED STATES
Email address: `gkorpal@arizona.edu`