Finding pairs of primes with small order reciprocity

Grad Student Algebra and Number Theory Seminar

Craig Costello[1] **Gaurish Korpal**[2]

[1]Queensland University of Technology, Brisbane, Australia
craig.costello@qut.edu.au

[2]University of Arizona, Tucson, USA
gkorpal@arizona.edu

March 07, 2025

Outline

Outline

Order reciprocity

Prime pairs 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 $q^{k'} \equiv 1 \pmod{p}$.

`https://math.stackexchange.com/questions/3118453/order-reciprocity`

Outline

The two extremes - I

Theorem

Prime pairs with $(2, 2)$*-order reciprocity do not exist.*

The two extremes - I

Proof.

On the contrary, let $p < q$ be prime numbers such that $\mathrm{ord}_q(p) = 2 = \mathrm{ord}_p(q)$. Then $p \equiv -1 \pmod{q}$ and $q \equiv -1 \pmod{p}$. However, $p < q$ implies that $p = q - 1$, which forces $(p, q) = (2, 3)$ and $\mathrm{ord}_p(q) = 1$, a contradiction. $\square$

The two extremes - II

Theorem

There are infinitely many pairs (p, q) *that have* $(q-1, p-1)$*-order reciprocity.*

The two extremes - II

Proof.

A weaker form of Artin's conjecture for primitive roots[1] says that if there are three distinct prime numbers p_1, p_2, p_3, then at least one of them is a primitive root modulo q for infinitely many primes q. Therefore, at least one of the Fermat primes $p = 5, 17, 257$ is a primitive root (and thus a quadratic non-residue) modulo q for an infinite number of primes q. Since $p \equiv 1 \pmod 4$, by quadratic reciprocity, each such prime q is a non-residue modulo p. But for Fermat primes p, every non-residue q is automatically a primitive root[2]. In other words, for at least one $p \in \{5, 17, 257\}$, there exist infinitely many primes q such that $\operatorname{ord}_q(p) = q - 1$ and $\operatorname{ord}_p(q) = p - 1$. □

[1] D. R. Heath-Brown. "Artin's conjecture for primitive roots". In: *Quart. J. Math. Oxford Ser. (2)* 37.145 (1986), pp. 27–38, Corollary 1.

[2] M. Křížek, F. Luca, and L. Somer. *17 lectures on Fermat numbers*. Vol. 9. CMS Books in Mathematics/Ouvrages de Mathématiques de la SMC. Springer-Verlag, New York, 2001, Theorem 3.10.

The two extremes - II

Proof.

A weaker form of Artin's conjecture for primitive roots[1] says that if there are three distinct prime numbers p_1, p_2, p_3, then at least one of them is a primitive root modulo q for infinitely many primes q. Therefore, at least one of the Fermat primes $p = 5, 17, 257$ is a primitive root (and thus a quadratic non-residue) modulo q for an infinite number of primes q. Since $p \equiv 1 \pmod 4$, by quadratic reciprocity, each such prime q is a non-residue modulo p. But for Fermat primes p, every non-residue q is automatically a primitive root[2]. In other words, for at least one $p \in \{5, 17, 257\}$, there exist infinitely many primes q such that $\mathrm{ord}_q(p) = q - 1$ and $\mathrm{ord}_p(q) = p - 1$. □

[1] D. R. Heath-Brown. "Artin's conjecture for primitive roots". In: *Quart. J. Math. Oxford Ser. (2)* 37.145 (1986), pp. 27–38, Corollary 1.

[2] M. Křížek, F. Luca, and L. Somer. *17 lectures on Fermat numbers*. Vol. 9. CMS Books in Mathematics/Ouvrages de Mathématiques de la SMC. Springer-Verlag, New York, 2001, Theorem 3.10.

The two extremes - II

Proof.

A weaker form of Artin's conjecture for primitive roots[1] says that if there are three distinct prime numbers p_1, p_2, p_3, then at least one of them is a primitive root modulo q for infinitely many primes q. Therefore, at least one of the Fermat primes $p = 5, 17, 257$ is a primitive root (and thus a quadratic non-residue) modulo q for an infinite number of primes q. Since $p \equiv 1 \pmod 4$, by quadratic reciprocity, each such prime q is a non-residue modulo p. But for Fermat primes p, every non-residue q is automatically a primitive root[2]. In other words, for at least one $p \in \{5, 17, 257\}$, there exist infinitely many primes q such that $\mathrm{ord}_q(p) = q - 1$ and $\mathrm{ord}_p(q) = p - 1$. □

[1] D. R. Heath-Brown. "Artin's conjecture for primitive roots". In: *Quart. J. Math. Oxford Ser. (2)* 37.145 (1986), pp. 27–38, Corollary 1.

[2] M. Křížek, F. Luca, and L. Somer. *17 lectures on Fermat numbers*. Vol. 9. CMS Books in Mathematics/Ouvrages de Mathématiques de la SMC. Springer-Verlag, New York, 2001, Theorem 3.10.

The two extremes - II

Proof.

A weaker form of Artin's conjecture for primitive roots[1] says that if there are three distinct prime numbers p_1, p_2, p_3, then at least one of them is a primitive root modulo q for infinitely many primes q. Therefore, at least one of the Fermat primes $p = 5, 17, 257$ is a primitive root (and thus a quadratic non-residue) modulo q for an infinite number of primes q. Since $p \equiv 1 \pmod 4$, by quadratic reciprocity, each such prime q is a non-residue modulo p. But for Fermat primes p, every non-residue q is automatically a primitive root[2]. In other words, for at least one $p \in \{5, 17, 257\}$, there exist infinitely many primes q such that $\mathrm{ord}_q(p) = q - 1$ and $\mathrm{ord}_p(q) = p - 1$. □

[1] D. R. Heath-Brown. "Artin's conjecture for primitive roots". In: *Quart. J. Math. Oxford Ser. (2)* 37.145 (1986), pp. 27–38, Corollary 1.

[2] M. Křížek, F. Luca, and L. Somer. *17 lectures on Fermat numbers*. Vol. 9. CMS Books in Mathematics/Ouvrages de Mathématiques de la SMC. Springer-Verlag, New York, 2001, Theorem 3.10.

The two extremes - II

Proof.

A weaker form of Artin's conjecture for primitive roots[1] says that if there are three distinct prime numbers p_1, p_2, p_3, then at least one of them is a primitive root modulo q for infinitely many primes q. Therefore, at least one of the Fermat primes $p = 5, 17, 257$ is a primitive root (and thus a quadratic non-residue) modulo q for an infinite number of primes q. Since $p \equiv 1 \pmod 4$, by quadratic reciprocity, each such prime q is a non-residue modulo p. But for Fermat primes p, every non-residue q is automatically a primitive root[2]. In other words, for at least one $p \in \{5, 17, 257\}$, there exist infinitely many primes q such that $\mathrm{ord}_q(p) = q - 1$ and $\mathrm{ord}_p(q) = p - 1$. □

[1] D. R. Heath-Brown. "Artin's conjecture for primitive roots". In: *Quart. J. Math. Oxford Ser. (2)* 37.145 (1986), pp. 27–38, Corollary 1.

[2] M. Křížek, F. Luca, and L. Somer. *17 lectures on Fermat numbers*. Vol. 9. CMS Books in Mathematics/Ouvrages de Mathématiques de la SMC. Springer-Verlag, New York, 2001, Theorem 3.10.

MNT family

For $n \in \mathbb{Z}_{>0}$, the n-th *cyclotomic polynomial* $\Phi_n(x)$ is given by

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{d|n \\ d<n}} \Phi_d(x)}.$$

Theorem

Let p be a prime and $n, a \in \mathbb{Z}_{>0}$ such that $p \nmid na$. Then $\mathrm{ord}_p(a) = n$ iff $p \mid \Phi_n(a)$.

MNT family

Miyaji-Nakabayashi-Takano (MNT) family is parameterised as

$$p = \Phi_6(x) = x^2 - x + 1 \qquad \text{and} \qquad q = \Phi_4(x) = x^2 + 1,$$

from which it follows that $(k, k') = (\mathrm{ord}_q(p), \mathrm{ord}_p(q)) = (6, 4)$

Outline

Conditions

We are interested in instances of prime pairs where p and q are *large* (cryptographic size) and where k and k' are *small* (no larger than 50).

Algorithm outline

Recall that for a cyclic group $G = \langle g \rangle$ of order s, the order of $h = g^r$ is

$$\mathrm{ord}_G(h) = \frac{s}{\gcd(r, s)}$$

Then the following algorithm gives us all (k, k')-cycles such that $q < p$.

1. Choose a prime p such that $p \equiv 1 \pmod{k'}$. Let $\mathbb{F}_p^\times = \langle \alpha \rangle$ and set
   $$t = \frac{|\mathbb{F}_p^\times|}{k'} = \frac{p-1}{k'} < p - 1.$$
2. Compute the set $\mathcal{Q}_{k'}$ of prime numbers $q \equiv 1 \pmod{k}$ given by α^m with $\gcd(m, p-1) = t$.
3. $\mathrm{ord}_p(q) = k' \iff q \in \mathcal{Q}_{k'}$.
4. $\mathrm{ord}_q(p) = k \iff p^k \equiv 1 \pmod{q}$ but $p^d \not\equiv 1 \pmod{q}$ for $d \mid k$ and $d < k$.

If $k \neq k'$ then run it again by swapping k and k' to get complete list.

Algorithm outline

Recall that for a cyclic group $G = \langle g \rangle$ of order s, the order of $h = g^r$ is

$$\mathrm{ord}_G(h) = \frac{s}{\gcd(r, s)}$$

Then the following algorithm gives us all (k, k')-cycles such that $q < p$.

1. Choose a prime p such that $p \equiv 1 \pmod{k'}$. Let $\mathbb{F}_p^\times = \langle \alpha \rangle$ and set $t = \dfrac{|\mathbb{F}_p^\times|}{k'} = \dfrac{p-1}{k'} < p - 1$.
2. Compute the set $\mathcal{Q}_{k'}$ of prime numbers $q \equiv 1 \pmod{k}$ given by α^m with $\gcd(m, p-1) = t$.
3. $\mathrm{ord}_p(q) = k' \iff q \in \mathcal{Q}_{k'}$.
4. $\mathrm{ord}_q(p) = k \iff p^k \equiv 1 \pmod{q}$ but $p^d \not\equiv 1 \pmod{q}$ for $d \mid k$ and $d < k$.

If $k \neq k'$ then run it again by swapping k and k' to get complete list.

Algorithm outline

Recall that for a cyclic group $G = \langle g \rangle$ of order s, the order of $h = g^r$ is

$$\mathrm{ord}_G(h) = \frac{s}{\gcd(r, s)}$$

Then the following algorithm gives us all (k, k')-cycles such that $q < p$.

1. Choose a prime p such that $p \equiv 1 \pmod{k'}$. Let $\mathbb{F}_p^\times = \langle \alpha \rangle$ and set $t = \dfrac{|\mathbb{F}_p^\times|}{k'} = \dfrac{p-1}{k'} < p - 1$.
2. Compute the set $\mathcal{Q}_{k'}$ of prime numbers $q \equiv 1 \pmod{k}$ given by α^m with $\gcd(m, p-1) = t$.
3. $\mathrm{ord}_p(q) = k' \iff q \in \mathcal{Q}_{k'}$.
4. $\mathrm{ord}_q(p) = k \iff p^k \equiv 1 \pmod{q}$ but $p^d \not\equiv 1 \pmod{q}$ for $d \mid k$ and $d < k$.

If $k \neq k'$ then run it again by swapping k and k' to get complete list.

Algorithm outline

Recall that for a cyclic group $G = \langle g \rangle$ of order s, the order of $h = g^r$ is

$$\mathrm{ord}_G(h) = \frac{s}{\gcd(r, s)}$$

Then the following algorithm gives us all (k, k')-cycles such that $q < p$.

1. Choose a prime p such that $p \equiv 1 \pmod{k'}$. Let $\mathbb{F}_p^\times = \langle \alpha \rangle$ and set $t = \dfrac{|\mathbb{F}_p^\times|}{k'} = \dfrac{p-1}{k'} < p - 1$.
2. Compute the set $\mathcal{Q}_{k'}$ of prime numbers $q \equiv 1 \pmod{k}$ given by α^m with $\gcd(m, p-1) = t$.
3. $\mathrm{ord}_p(q) = k' \iff q \in \mathcal{Q}_{k'}$.
4. $\mathrm{ord}_q(p) = k \iff p^k \equiv 1 \pmod{q}$ but $p^d \not\equiv 1 \pmod{q}$ for $d \mid k$ and $d < k$.

If $k \neq k'$ then run it again by swapping k and k' to get complete list.

Algorithm outline

Recall that for a cyclic group $G = \langle g \rangle$ of order s, the order of $h = g^r$ is

$$\mathrm{ord}_G(h) = \frac{s}{\gcd(r, s)}$$

Then the following algorithm gives us all (k, k')-cycles such that $q < p$.

1. Choose a prime p such that $p \equiv 1 \pmod{k'}$. Let $\mathbb{F}_p^\times = \langle \alpha \rangle$ and set $t = \dfrac{|\mathbb{F}_p^\times|}{k'} = \dfrac{p-1}{k'} < p - 1$.
2. Compute the set $\mathcal{Q}_{k'}$ of prime numbers $q \equiv 1 \pmod{k}$ given by α^m with $\gcd(m, p-1) = t$.
3. $\mathrm{ord}_p(q) = k' \iff q \in \mathcal{Q}_{k'}$.
4. $\mathrm{ord}_q(p) = k \iff p^k \equiv 1 \pmod{q}$ but $p^d \not\equiv 1 \pmod{q}$ for $d \mid k$ and $d < k$.

If $k \neq k'$ then run it again by swapping k and k' to get complete list.

Algorithm outline

Recall that for a cyclic group $G = \langle g \rangle$ of order s, the order of $h = g^r$ is

$$\mathrm{ord}_G(h) = \frac{s}{\gcd(r, s)}$$

Then the following algorithm gives us all (k, k')-cycles such that $q < p$.

1. Choose a prime p such that $p \equiv 1 \pmod{k'}$. Let $\mathbb{F}_p^\times = \langle \alpha \rangle$ and set $t = \dfrac{|\mathbb{F}_p^\times|}{k'} = \dfrac{p-1}{k'} < p - 1$.
2. Compute the set $\mathcal{Q}_{k'}$ of prime numbers $q \equiv 1 \pmod{k}$ given by α^m with $\gcd(m, p-1) = t$.
3. $\mathrm{ord}_p(q) = k' \iff q \in \mathcal{Q}_{k'}$.
4. $\mathrm{ord}_q(p) = k \iff p^k \equiv 1 \pmod{q}$ but $p^d \not\equiv 1 \pmod{q}$ for $d \mid k$ and $d < k$.

If $k \neq k'$ then run it again by swapping k and k' to get complete list.

Algorithm outline

Recall that for a cyclic group $G = \langle g \rangle$ of order s, the order of $h = g^r$ is

$$\mathrm{ord}_G(h) = \frac{s}{\gcd(r, s)}$$

Then the following algorithm gives us all (k, k')-cycles such that $q < p$.

1. Choose a prime p such that $p \equiv 1 \pmod{k'}$. Let $\mathbb{F}_p^\times = \langle \alpha \rangle$ and set $t = \dfrac{|\mathbb{F}_p^\times|}{k'} = \dfrac{p-1}{k'} < p - 1$.
2. Compute the set $\mathcal{Q}_{k'}$ of prime numbers $q \equiv 1 \pmod{k}$ given by α^m with $\gcd(m, p-1) = t$.
3. $\mathrm{ord}_p(q) = k' \iff q \in \mathcal{Q}_{k'}$.
4. $\mathrm{ord}_q(p) = k \iff p^k \equiv 1 \pmod{q}$ but $p^d \not\equiv 1 \pmod{q}$ for $d \mid k$ and $d < k$.

If $k \neq k'$ then run it again by swapping k and k' to get complete list.

Data

P_1 be the list of first 100 million primes and P_2 be the list of the next 100 million primes.

Table: Counts of prime pairs with selected (k, k')-order reciprocity.

(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

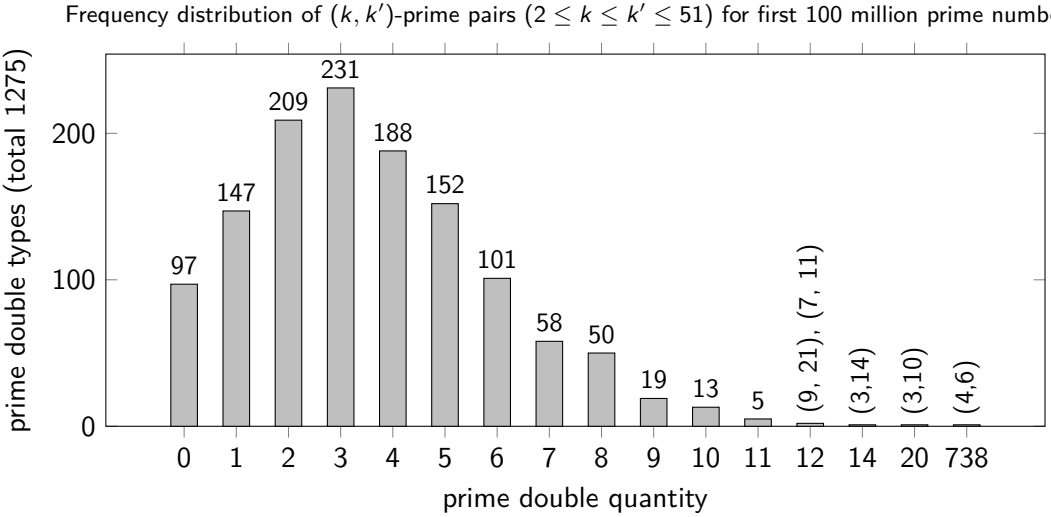
Data

P_1 be the list of first 100 million primes and P_2 be the list of the next 100 million primes.

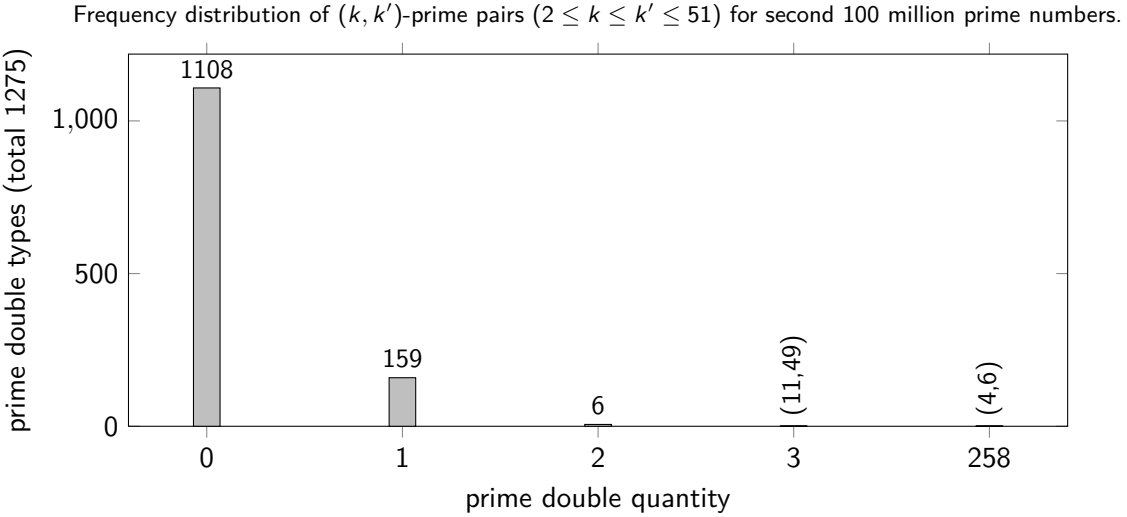
Table: The number of (k, k') corresponding to various frequencies of prime pairs.

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

Data


Frequency distribution of (k, k')-prime pairs $(2 \leq k \leq k' \leq 51)$ for first 100 million prime numbers.
prime double types (total 1275)
0
100
200
97
147
209
231
188
152
101
58
50
19
13
5
(9, 21), (7, 11)
(3,14)
(3,10)
(4,6)
0 1 2 3 4 5 6 7 8 9 10 11 12 14 20 738
prime double quantity

Data


Frequency distribution of (k, k')-prime pairs $(2 \leq k \leq k' \leq 51)$ for second 100 million prime numbers.
prime double types (total 1275)
1,000
500
0
1108
159
6
(11,49)
(4,6)
0
1
2
3
258
prime double quantity

Outline

Wishlist

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

Wishlist

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

Wishlist

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

Wishlist

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