#A7 INTEGERS 12 (2012)

A PROPERTY OF TWIN PRIMES

Christian Aebi
Collège Calvin, Geneva, Switzerland
christian.aebi@edu.ge.ch

Grant Cairns
Department of Mathematics, La Trobe University, Melbourne, Australia
G.Cairns@latrobe.edu.au

Received: 2/8/11, Accepted: 12/19/11, Published: 1/2/12

Abstract

We determine the product of the invertible quadratic residues in $\mathbb{Z}_n$. This is a variation on Gauss' generalization of Wilson's Theorem. From this we deduce that for twin primes $p, p+2$, the product of the invertible quadratic residues in $\mathbb{Z}_{p(p+2)}$ is $\pm(p+1)$, where the sign depends on the residue class of p modulo 4. We examine necessary and sufficient conditions for consecutive odd natural numbers $m, m+2$ to satisfy this property of twin primes. The paper concludes with two open questions.

1. Introduction

Wilson's theorem can be expressed as follows: if n is a natural number, then n is prime if and only if

$$\prod_{s\in\mathbb{Z}_n\setminus\{0\}} s \equiv -1 \pmod{n}.$$

Gauss' generalization of Wilson's Theorem states that if I denotes the set of invertible elements in $\mathbb{Z}_n$, then

$$\prod_{s\in I} s \equiv \begin{cases} -1 & : \text{ if } n = 4, p^\alpha, 2p^\alpha \ (p \text{ an odd prime}) \\ \ \ 1 & : \text{ otherwise} \end{cases} \pmod{n}.$$

Gauss stated this in [6, art. 78], writing "For the sake of brevity we omit the proof and only observe that it can be done as in the preceding article [which gave a proof of one direction of Wilson's theorem] except that the congruence $x^2 \equiv 1$ can have more than two roots, which require some special considerations." According to [5, Chap. III], proofs of Gauss' generalization of Wilson's Theorem were provided by Minding (1832), Brennecke (1839), Crelle (1840), Prouhet (1845), Arndt (1846), Dirichlet (1863), Schering (1882), Daniels (1890) and Kronecker (1901). Then in 1903, Miller gave a very elegant proof using group theory [7].

Several generalizations of the Gauss-Wilson theorem have been given [2, 9, 3, 4]. Our generalization looks at the product of the invertible quadratic residues. Suppose that n is a natural number, I is the set of invertible elements in $\mathbb{Z}_n$ and R is the set of quadratic residues (i.e., squares) in $\mathbb{Z}_n$. We prove:

Theorem 1. *If $n \in \mathbb{N}$ has prime decomposition $n = p_1^{r_1} \cdots p_k^{r_k}$, then $\prod_{s \in I \cap R} s \equiv 1 \pmod{n}$ unless there is precisely one prime p_i with $p_i \equiv 1 \pmod 4$, and in this case $\prod_{s \in I \cap R} s$ is congruent modulo n to the unique element of $\mathbb{Z}_n$ that is congruent to -1 modulo $p_i^{r_i}$ and congruent to 1 modulo $n/p_i^{r_i}$.*

This result generalizes the well-known fact that if $n = p$ is prime, the product of the invertible quadratic residues is $-1 \pmod{p}$ if and only if $p \equiv 1 \pmod 4$; see [8, p. 75] for example.

Suppose that $p, p+2$ are twin primes and let $n = p(p+2)$. Then the following condition holds:

$$\prod_{s \in I \cap R} s \equiv (p+1) \cdot (-1)^{\frac{p+1}{2}} \pmod{p(p+2)}. \tag{C}$$

Indeed, condition (C) can be deduced from Theorem 1 or alternately, it can be established directly in 5 easy steps:

1. As p and $q := p+2$ are prime, the only elements that are their own inverse in $\mathbb{Z}_{pq}$ are $\pm 1, \pm(p+1)$.
2. Each invertible square will have a distinct inverse which is also a square, except those that are their own inverse.
3. -1 is not a square in $\mathbb{Z}_{pq}$ because -1 will be square in $\mathbb{Z}_p$ or in $\mathbb{Z}_q$ but not in both.
4. $p+1$ is a square in $\mathbb{Z}_p$, and if $q \equiv 1 \pmod 4$ then $p+1$ is a square in $\mathbb{Z}_q$, therefore also in $\mathbb{Z}_{pq}$. Similarly, $(-p-1)$ is square in $\mathbb{Z}_q$, and if $p \equiv 1 \pmod 4$ then $-p-1$ is a square in $\mathbb{Z}_p$, therefore also in $\mathbb{Z}_{pq}$
5. So either $p+1$ or $-p-1$ is a square in $\mathbb{Z}_{pq}$, and the product of all the invertible squares equals the square in question.

The main purpose of this note is to determine which consecutive odd natural numbers p, $p+2$ verify condition (C). This follows considerations of related questions in [1]. As before, let I (resp. R) denote the set of invertible elements (resp. quadratic residues) in $\mathbb{Z}_{p(p+2)}$. We have:

Theorem 2. *Let $p > 1$ be a natural number. Condition (C) holds if and only if one of the following conditions holds:*

(a) $p = q^k$ *where* q *is prime and* $q \equiv 1 \pmod 4$*, and each of the prime divisors of* $p+2$ *is congruent to* $3 \pmod 4$*,*

(b) $p+2 = q^k$ *where* q *is prime and* $q \equiv 1 \pmod 4$*, and each of the prime divisors of* p *is congruent to* $3 \pmod 4$*.*

Note that if condition (a) holds, then $p \equiv 1 \pmod 4$ and so $p+2 \equiv 3 \pmod 4$; thus, as the prime divisors of $p+2$ are each congruent to $3 \pmod 4$, the sum of the exponents in the prime decomposition of $p+2$ is odd. Similarly, if condition (b) holds, the sum of the exponents in the prime decomposition of p is odd.

2. Preliminaries and Proof of Theorem 1

Let n be an odd natural number, let $n = p_1^{r_1} \cdots p_k^{r_k}$ be its prime decomposition and let $K = \{1, \ldots, k\}$ be the set of indices.

Lemma 3. *There are* 2^k *solutions to the equation* $x^2 = 1$ *in* $\mathbb{Z}_n$*. For* $S = K$*, set* $x_S := 1$*. If* S *is a proper subset of* K*, let* S' *denote the complement of* S *in* K*, let* $\overline{S} = \prod_{i \in S} p_i^{r_i}$*, let* $\overline{S}^{-1}$ *denote the smallest positive residue of the multiplicative inverse of* $\overline{S}$ *in* $\mathbb{Z}_{\overline{S'}}$*, and finally set*

$$x_S := -2 \cdot \overline{S}^{-1} \cdot \overline{S} + 1.$$

Then $\{x_S : S \subseteq K\}$ *is the set of solutions of* $x^2 = 1$ *in* $\mathbb{Z}_n$*.*

Remark 4. For $S \neq K$, note that $x_S - 1$ is divisible by $\overline{S}$ and $x_S + 1 = 2(1 - \overline{S}^{-1} \cdot \overline{S})$, which is a multiple of $\overline{S'}$. So $x_S \equiv 1 \pmod{\overline{S}}$ and $x_S \equiv -1 \pmod{\overline{S'}}$. Thus $x_S \equiv 1 \pmod{p_i}$ for all $i \in S$ and $x_S \equiv -1 \pmod{p_i}$ for all $i \in S'$. In particular, the x_S are distinct. Note that for S equal to the empty set, $\overline{S} = 1, \overline{S'} = n$ and $\overline{S}^{-1} = 1$, so $x_S = -1$.

Proof of Lemma 3. If $x^2 = 1$ in $\mathbb{Z}_n$, then for each prime p_i, for $i = 1, \ldots, k$, we have $x \equiv \pm 1 \pmod{p_i^{r_i}}$. For each choice of $S \subseteq K$, the Chinese remainder theorem gives a unique solution x in $\mathbb{Z}_n$ for which $x \equiv 1 \pmod{p_i^{r_i}}$ for all $i \in S$ and $x \equiv -1 \pmod{p_i^{r_i}}$ for all $i \in S'$. Conversely, if x satisfies this condition, then $x - 1$ is divisible by p_i for all $i \in S$ and $x + 1$ is divisible by p_i for all $i \in S'$, and thus $x^2 - 1 = (x-1)(x+1)$ is zero in $\mathbb{Z}_n$. So there are precisely 2^k solutions to the equation $x^2 = 1$ in $\mathbb{Z}_n$, one for each subset $S \subseteq K$. □

Note that x_S is a quadratic residue in $\mathbb{Z}_n$ if and only if x_S is a quadratic residue in $\mathbb{Z}_{p_i}$ for all $i \in K$. Moreover, -1 is a quadratic residue in $\mathbb{Z}_{p_i}$ if and only if $p_i \equiv 1 \pmod 4$. Thus, since $x_S \equiv 1 \pmod{p_i}$ for all $i \in S$ and $x_S \equiv -1 \pmod{p_i}$ for all $i \in S'$, we have the following result, which we record as a lemma.

Lemma 5. *x_S is a quadratic residue in $\mathbb{Z}_n$ if and only if $p_i \equiv 1 \pmod 4$ for all $i \in S'$.*

Lemma 6. *The following conditions are equivalent:*

(a) *There is exactly one proper subset S of K such that x_S is a quadratic residue in $\mathbb{Z}_n$.*

(b) *There is exactly one element $i \in K$ with $p_i \equiv 1 \pmod 4$.*

Proof. By Lemma 5, the subsets $S \subseteq K, S \neq K$, such that x_S is a quadratic residue are precisely the complements of the nonempty subsets of $\{i \in K : p_i \equiv 1 \pmod 4\}$. □

Proof of Theorem 1. Let J denote the subset of R of elements that are their own inverse in $\mathbb{Z}_n$. Clearly,

$$\prod_{s \in I \cap R} s = \prod_{s \in J} s.$$

Notice that J forms a subgroup of the multiplicative group of $\mathbb{Z}_n$. Moreover, each element of J has order 2. But it is a general fact that in a finite Abelian group in which each element has order 2, the product of the elements is 1 unless the group has order 2; i.e., it has only one non trivial element. In the latter case, by Lemma 6 and its proof, there is exactly one element $i \in K$ with $p_i \equiv 1 \pmod 4$ and $\prod_{s \in J} s = x_S$, where $S = K \backslash \{i\}$. By Remark 4, x_S is the unique element of $\mathbb{Z}_n$ that is congruent to -1 modulo $p_i^{r_i}$ and congruent to 1 modulo $n/p_i^{r_i}$. This completes the proof. □

3. Proof of Theorem 2

We will give the proof in the case where $p \equiv 3 \pmod 4$. The other case is treated in an entirely analogous manner.

Let $p_1^{r_1} \cdots p_k^{r_k}$ be the prime decomposition of $n := p(p+2)$ and let $K = \{1, \ldots, k\}$. Let P (resp. Q) be the set of elements $i \in K$ for which p_i is a divisor of p (resp. $p+2$); so $P \cap Q = \emptyset$ and $P \cup Q = K$. Note that $\overline{P} = p, \overline{Q} = p+2$ and $x_P \equiv p+1 \pmod n$. Indeed, by Lemma 3, x_P is the unique element that is congruent to 1 modulo p and -1 modulo $p+2$, and $p+1$ has these properties. As in the proof of Theorem 1, let J denote the subset of R of elements that are their own inverse in $\mathbb{Z}_n$. So $\prod_{s \in I \cap R} s = \prod_{s \in J} s$.

We now show that conditions (a) and (b) of the theorem are sufficient. In fact, case (a) does not occur when $p \equiv 3 \pmod 4$. In case (b), by Lemma 6, P is the only proper subset of K such that x_P is a quadratic residue in $\mathbb{Z}_n$. As we observed above, $x_P \equiv p+1 \pmod n$. So, as $(-1)^{\frac{p+1}{2}} = 1$, condition (C) holds.

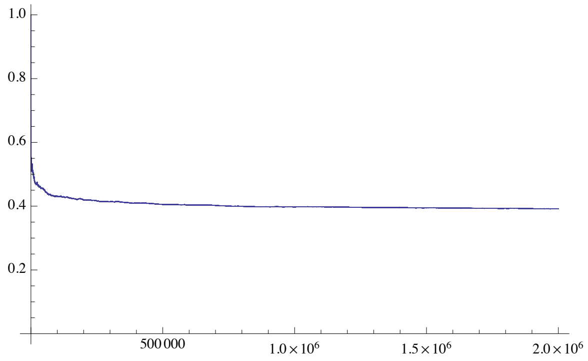

Figure 1: T_n/C_n for $n \leq 2,000,000$

Conversely, suppose that condition (C) holds, so $\prod_{s \in I \cap R} s = p+1$. From Theorem 1, there is a unique prime p_i with $p_i \equiv 1 \pmod 4$, and in this case $\prod_{s \in I \cap R} s$ is congruent modulo n to the unique element of $\mathbb{Z}_n$ that is congruent to -1 modulo $p_i^{r_i}$ and congruent to 1 modulo $n/p_i^{r_i}$. Thus there exists $a, b \in \mathbb{N}$ such that

$$p+1 = -1 + ap_i^{r_i}, \tag{1}$$

$$p+1 = 1 + bn/p_i^{r_i}. \tag{2}$$

Now, (1) gives $p+2 = ap_i^{r_i}$ and using this, (2) gives $p = bn/p_i^{r_i} = abp$. Hence $a = b = 1$, and so $p+2 = p_i^{r_i}$. This establishes condition (b) and completes the proof.

4. Two Questions

There are two obvious questions:

Question 1. Are there infinitely many odd natural numbers p for which condition (C) holds?

Given $n \in \mathbb{N}$, let T_n denote the number of primes $p < n$ for which $p+2$ is prime, and let C_n denote the number of odd natural numbers $p < n$ for which condition (C) holds.

Question 2. Is $\lim\limits_{n\to\infty} \dfrac{T_n}{C_n}$ strictly positive?

Figure 1 shows values of T_n/C_n for $n \leq$ 2,000,000, calculated using Mathematica.

References

[1] Christian Aebi and Grant Cairns, Catalan numbers, primes, and twin primes, Elem. Math. **63** (2008), no. 4, 153–164.

[2] L. Carlitz, A note on the generalized Wilson's theorem, Amer. Math. Monthly **71** (1964), 291–293.

[3] John B. Cosgrave and Karl Dilcher, Extensions of the Gauss-Wilson theorem, Integers **8** (2008), A39, 15pp.

[4] Chandan Singh Dalawat, Wilson's theorem, J. Théor. Nombres Bordeaux **21** (2009), no. 3, 517–521.

[5] Leonard Eugene Dickson, History of the Theory of Numbers. Vol. I: Divisibility and primality., Chelsea Publishing Co., New York, 1966.

[6] Carl Friedrich Gauss, Disquisitiones Arithmeticae, Springer-Verlag, New York, 1986, Translated and with a preface by Arthur A. Clarke, Revised by William C. Waterhouse, Cornelius Greither and A. W. Grootendorst and with a preface by Waterhouse.

[7] G. A. Miller, A new proof of the generalized Wilson's theorem, Ann. of Math. (2) **4** (1903), no. 4, 188–190.

[8] H. E. Rose, A Course in Number Theory, second ed., Oxford Science Publications, The Clarendon Press Oxford University Press, New York, 1994.

[9] Štefan Schwarz, The role of semigroups in the elementary theory of numbers, Math. Slovaca **31** (1981), no. 4, 369–395.