involve
a journal of mathematics

Sophie Germain primes and involutions of $\mathbb{Z}_n^\times$

Karenna Genzlinger and Keir Lockridge

msp

2015 vol. 8, no. 4

INVOLVE 8:4 (2015)
dx.doi.org/10.2140/involve.2015.8.653

Sophie Germain primes and involutions of $\mathbb{Z}_n^\times$

Karenna Genzlinger and Keir Lockridge

(Communicated by Kenneth S. Berenhaut)

In the paper "What is special about the divisors of 24?", Sunil Chebolu proved an interesting result about the multiplication tables of $\mathbb{Z}_n$ from several different number theoretic points of view: all of the 1s in the multiplication table for $\mathbb{Z}_n$ are located on the main diagonal if and only if n is a divisor of 24. Put another way, this theorem characterizes the positive integers n with the property that the proportion of 1s on the diagonal is precisely 1. The present work is concerned with finding the positive integers n for which there is a given fixed proportion of 1s on the diagonal. For example, when p is prime, we prove that there exists a positive integer n such that $1/p$ of the 1s lie on the diagonal of the multiplication table for $\mathbb{Z}_n$ if and only if p is a Sophie Germain prime.

1. Introduction

Let R be a ring and let $R^\times$ denote its group of units. Call a unit u in $R^\times$ a *diagonal unit* if the multiplicative order of u is at most 2. Such units are more commonly referred to as involutions; our motivation for calling them diagonal units is as follows. The units of R are in one-to-one correspondence with 1s appearing in its multiplication table, and the diagonal units are in one-to-one correspondence with the 1s appearing on the diagonal. When the order of $R^\times$ is finite, we will write $\mathrm{du}(R)$ for the number of diagonal units and

$$\mathrm{pdu}(R) = \frac{\mathrm{du}(R)}{|R^\times|}$$

MSC2010: primary 11A41; secondary 16U60.
Keywords: Sophie Germain primes, group of units, Gauss–Wantzel theorem.

for the proportion of diagonal units in $R^\times$. We will only consider commutative rings, in which case $R^\times$ is an abelian group. This means that the units of order at most 2 form a subgroup of $R^\times$. Hence, $\mathrm{du}(R)$ divides $|R^\times|$ by Lagrange's theorem, so $\mathrm{pdu}(R)$ is always the reciprocal of an integer. We therefore find it more convenient to work with the *ratio of diagonal units*,

$$\mathrm{rdu}(R) = \frac{|R^\times|}{\mathrm{du}(R)} = \frac{1}{\mathrm{pdu}(R)}.$$

For brevity, we will write $\mathrm{du}(n)$, $\mathrm{pdu}(n)$ and $\mathrm{rdu}(n)$ for the quantities $\mathrm{du}(\mathbb{Z}_n)$, $\mathrm{pdu}(\mathbb{Z}_n)$, and $\mathrm{rdu}(\mathbb{Z}_n)$.

A ring R is said to *satisfy the diagonal property* if every unit of R is a diagonal unit; that is, R satisfies the diagonal property if and only if $\mathrm{pdu}(R) = \mathrm{rdu}(R) = 1$. Chebolu [2012] proved that $\mathbb{Z}_n$ satisfies the diagonal property if and only if n is a divisor of 24. This leads naturally to a more general study of the equation

$$\mathrm{rdu}(n) = \theta, \tag{1}$$

where $\theta \geq 1$. For which values of θ does (1) have a solution? If (1) has a solution, can we find the entire solution set? We will answer both of these questions in several cases in Section 4. For example, we will prove the following theorem, which answers both questions when θ is prime.

Theorem 1.1. *Let p be a prime. There exists a positive integer n such that the proportion of diagonal units in $\mathbb{Z}_n$ is $1/p$ if and only if p is a Sophie Germain prime. For a Sophie Germain prime p, the set of solutions to* $\mathrm{rdu}(n) = p$ *is*

$$\begin{aligned}
(2p+1)\cdot\{\textit{divisors of } 24\} \quad &\textit{if } p > 3,\\
(2p+1)\cdot\{\textit{divisors of } 24\} \cup\ p^2\cdot\{\textit{divisors of } 8\} \quad &\textit{if } p = 3,\\
(2p+1)\cdot\{\textit{divisors of } 24\} \cup\ p^4\cdot\{\textit{divisors of } 3\} \quad &\textit{if } p = 2.
\end{aligned}$$

A Sophie Germain prime is a prime p such that $2p+1$ is also prime, in which case $2p+1$ is called a safe prime. Such primes arose in Marie-Sophie Germain's considerable work on Fermat's last theorem (see [Laubenbacher and Pengelley 1999]).

The remainder of this paper is organized as follows. Section 2 includes background information and a formula for the ratio of diagonal units. We then prove in Section 3 that the equation $\mathrm{rdu}(n) = \theta$ has a solution if and only if θ admits a special type of factorization, and we provide a principle for organizing solutions to this equation given a list of these factorizations. Section 4 is devoted to examples, including proofs of Chebolu's 24 theorem and Theorem 1.1. We also explore a surprising connection between the proportion of diagonal units and the Gauss–Wantzel theorem on the constructibility of regular polygons (Theorem 4.2). In the last section, we consider a generalization of the current situation and examine 1s on the diagonal of the multiplication cube for $\mathbb{Z}_n$.

2. The ratio of diagonal units

A common concept in number theory is the notion of a multiplicative function. A function $f : \mathbb{Z}^+ \to \mathbb{Z}^+$ is *multiplicative* if $f(st) = f(s)f(t)$ whenever s and t are relatively prime. Euler's totient function is an example of a multiplicative function par excellence (see [Burton 1989, §7]); it counts the positive integers $k \le n$ that are relatively prime to n. The relevant properties of $\phi(n)$ are summarized in the next theorem.

Theorem 2.1 (Euler's totient function). *Let $\phi(n)$ denote the number of positive integers less than n and relatively prime to n.*

(A) *The order of $\mathbb{Z}_n^\times$ is precisely $\phi(n)$.*

(B) *The function $\phi(n)$ is multiplicative.*

(C) *For any prime p and positive integer k, we have $\phi(p^k) = p^{k-1}(p-1)$.*

We now prove that the functions defined in Section 1 are multiplicative.

Proposition 2.2. *The functions* $\mathrm{du}(n)$, $\mathrm{pdu}(n)$, *and* $\mathrm{rdu}(n)$ *are multiplicative.*

Proof. Certainly, $\mathrm{rdu}(n)$ is multiplicative if and only if $\mathrm{pdu}(n)$ is multiplicative. Since $\mathrm{rdu}(n) = |\mathbb{Z}_n^\times| / \mathrm{du}(n) = \phi(n)/\mathrm{du}(n)$ and ϕ is multiplicative by the previous theorem, it suffices to prove that $\mathrm{du}(n)$ is multiplicative.

Let s and t be relatively prime positive integers. By the Chinese remainder theorem, $\mathbb{Z}_{st} \cong \mathbb{Z}_s \times \mathbb{Z}_t$. Since the order of $(x, y) \in \mathbb{Z}_s \times \mathbb{Z}_t$ is the least common multiple of the orders of x and y, the pair (x, y) is a diagonal unit if and only if x and y are diagonal units. Thus, $\mathrm{du}(st) = \mathrm{du}(s)\,\mathrm{du}(t)$. □

Our next goal is to give a formula for $\mathrm{rdu}(n)$. To do so, we need one more ingredient.

Theorem 2.3 (isomorphism class of $\mathbb{Z}_n^\times$). *For any integer $k \ge 1$ and odd prime p,*

$$\mathbb{Z}_{p^k}^\times \cong \mathbb{Z}_{\phi(p^k)} = \mathbb{Z}_{p^{k-1}(p-1)},$$

and

$$\mathbb{Z}_{2^k}^\times \cong \begin{cases} \{1\} & \text{if } k = 1, \\ \mathbb{Z}_2 & \text{if } k = 2, \\ \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}} & \text{if } k \ge 3. \end{cases}$$

The odd primary case is a consequence of the primitive root theorem; see [Cohen 2007, 2.1.24] for a short, fairly self-contained proof.

The next proposition provides a formula for the ratio of diagonal units in $\mathbb{Z}_n$.

Proposition 2.4. *Let n be a positive integer.*

(A) *For any odd prime p and integer $k \ge 1$,*

$$\mathrm{rdu}(p^k) = \phi(p^k)/2 = p^{k-1}(p-1)/2.$$

(B) *For any integer* $k \geq 0$,

$$\operatorname{rdu}(2^k) = \begin{cases} 1 & \text{if } k = 0, 1, 2, \text{ or } 3, \\ 2^{k-3} & \text{if } k > 3. \end{cases}$$

(C) *Let* $n = 2^a 3^b n'$, *where* $a, b \geq 0$ *and* $(n', 6) = 1$. *Let* r *denote the number of distinct primes dividing* n'. *Then*,

$$\operatorname{rdu}(n) = \begin{cases} \phi(n')/2^r & \text{if } a \leq 3,\ b \leq 1, \\ 2^{a-3}\phi(n')/2^r & \text{if } a > 3,\ b \leq 1, \\ 3^{b-1}\phi(n')/2^r & \text{if } a \leq 3,\ b > 1, \\ 2^{a-3}3^{b-1}\phi(n')/2^r & \text{if } a > 3,\ b > 1. \end{cases}$$

Proof. By Theorem 2.1(A), $\operatorname{rdu}(n) = \phi(n)/\operatorname{du}(n)$. Next observe that $\operatorname{du}(2) = 1$, $\operatorname{du}(4) = 2$, $\operatorname{du}(2^k) = 4$ for $k \geq 3$, and $\operatorname{du}(p^k) = 2$ for any odd prime p by Theorem 2.3 (for the last case, note that the group of units is cyclic of even order, so it has a unique subgroup of order 2). Combining these facts with the formula for $\phi(p^k)$ given in Theorem 2.1(C), one obtains parts (A) and (B). Part (C) follows from the previous two parts and the fact that $\operatorname{rdu}(n)$ is multiplicative. □

Though it is likely no surprise that the prime 2 is isolated in Proposition 2.4(C), our reason for isolating the prime 3 may be unclear. For now, we hope the reader is content with the observation that 2 and 3 are the only prime divisors of 24. In slightly more detail, the issue has to do with the fact that if $p > 3$ is prime, then $\operatorname{rdu}(p^k) = p$ is impossible, but $\operatorname{rdu}(3^2) = 3$ and $\operatorname{rdu}(2^4) = 2$. Note further that $\operatorname{rdu}(p^k)$ in Proposition 2.4(A) factors as $\theta(2\theta + 1)^k$, where $2\theta + 1$ is prime. This hints at the relevance of Sophie Germain primes, which appeared in Theorem 1.1, and leads to the study of positive integers that admit the special type of factorization discussed in the following section.

3. Sophie Germain factorizations

Given a positive integer θ, a *Sophie Germain factorization* of θ is a triple

$$F = (s, t, \{(\theta_1, \beta_1), \ldots, (\theta_r, \beta_r)\}),$$

where

(A) $\theta = |F| = 2^s 3^t \prod_{i=1}^{r} \theta_i (2\theta_i + 1)^{\beta_i}$,

(B) $s \geq 0$ and $t \geq 0$;

(C) for $i = 1, \ldots, r$, $\beta_i \geq 0$ and $\theta_i > 1$; and

(D) the integers $2\theta_1 + 1, \ldots, 2\theta_r + 1$ are distinct primes.

When $r = 0$, the set in the third coordinate of F is empty and the indexed product in (A) is 1. The ordered triple gives the data for the factorization, but the definition

of $|F|$ gives a far more readable interpretation of what the data represent. We will therefore abuse notation and use the expression defining $|F|$ in place of F itself. There is some ambiguity, however, since θ_i can be 2 or 3; consequently, we will always include the exponents s and t unsimplified, even when $s = 1$ or $t = 1$, unless either is equal to zero, in which case we will omit the corresponding factor entirely. We will not omit zero exponents in the indexed product, and the empty product will appear as 1. For clarification, here are several examples:

$$\begin{aligned} |(0,0,\varnothing)| &= 1, \\ |(0,0,\{(3,0)\})| &= 3\cdot 7^0, \\ |(0,1,\varnothing)| &= 3^1\cdot 1, \\ |(5,1,\{(3,0),(5,2),(9,4)\})| &= 2^5\cdot 3^1\cdot 3\cdot 7^0\cdot 5\cdot 11^2\cdot 9\cdot 19^4. \end{aligned}$$

The main difficulty of our current undertaking is to find all possible such factorizations of a given positive integer. However, given a list of the Sophie Germain factorizations of $\mathrm{rdu}(n)$, we will see at the end of this section that it is easy to find all solutions to (1).

Let $\mathcal{S}$ denote the set of all Sophie Germain factorizations of positive integers. We next define two functions,

$$\mathcal{F}:\mathbb{Z}^+\to\mathcal{S}$$

and

$$\mathcal{N}:\mathcal{S}\to\mathbb{Z}^+.$$

The function $\mathcal{F}(n)$ will select a canonical Sophie Germain factorization of n, and the function $\mathcal{N}(F)$ will select a positive integer whose canonical Sophie Germain factorization is F. Let

$$\mathcal{F}\Big(2^a3^b\prod_{i=1}^r p_i^{\alpha_i}\Big)=\begin{cases}\prod_{i=1}^r((p_i-1)/2)\cdot p_i^{\alpha_i-1} & \text{if } a\le 3,\ b\le 1,\ (1)\\ 2^{a-3}\cdot\prod_{i=1}^r((p_i-1)/2)\cdot p_i^{\alpha_i-1} & \text{if } a>3,\ b\le 1,\ (2)\\ 3^{b-1}\cdot\prod_{i=1}^r((p_i-1)/2)\cdot p_i^{\alpha_i-1} & \text{if } a\le 3,\ b>1,\ (3)\\ 2^{a-3}3^{b-1}\cdot\prod_{i=1}^r((p_i-1)/2)\cdot p_i^{\alpha_i-1} & \text{if } a>3,\ b>1,\ (4)\end{cases}$$

and let

$$\mathcal{N}\Big(2^s3^t\cdot\prod_{i=1}^r\theta_i(2\theta_i+1)^{\beta_i}\Big)=\begin{cases}\prod_{i=1}^r(2\theta_i+1)^{\beta_i+1} & \text{if } s=0,\ t=0,\\ 2^{s+3}\cdot\prod_{i=1}^r(2\theta_i+1)^{\beta_i+1} & \text{if } s>0,\ t=0,\\ 3^{t+1}\cdot\prod_{i=1}^r(2\theta_i+1)^{\beta_i+1} & \text{if } s=0,\ t>0,\\ 2^{s+3}3^{t+1}\cdot\prod_{i=1}^r(2\theta_i+1)^{\beta_i+1} & \text{if } s>0,\ t>0,\end{cases}$$

The indexed product in the definition of $\mathcal{F}$ is of course just $\phi(n')/2^r$, where $n'=n/(2^a3^b)$. In the definition of $\mathcal{F}$, we have labeled the cases 1–4. Every Sophie

Germain factorization falls into precisely one of these four cases, so we will use these numbers to refer to the *type* of a Sophie Germain factorization. If we were to only consider integers relatively prime to 6, the above formulas would each have a single case and these functions would be inverses; interference from the divisors of 24 causes a bit of trouble. We summarize the relevant properties of $\mathcal{F}$ and $\mathcal{N}$ in the following theorem.

Proposition 3.1. *Let $\mathcal{F} : \mathbb{Z}^+ \to \mathcal{S}$ and $\mathcal{N} : \mathcal{S} \to \mathbb{Z}^+$ be the functions defined above.*

(A) *For any positive integer n,* $\mathrm{rdu}(n) = |\mathcal{F}(n)|$.

(B) *For any Sophie Germain factorization F,*

$$\mathcal{F}(\mathcal{N}(F)) = F.$$

In particular, $\mathcal{F}$ is surjective.

Proof. The verification of each statement entails a straightforward computation using the definitions of $\mathcal{F}$ and $\mathcal{N}$ combined with Proposition 2.4(C). □

We now have the following general result.

Theorem 3.2. *Fix a positive integer θ. The equation*

$$\mathrm{rdu}(n) = \theta \tag{2}$$

has a solution if and only if θ admits a Sophie Germain factorization.

Proof. If (2) has a solution, then $\theta = |\mathcal{F}(n)|$, so θ admits a Sophie Germain factorization. Conversely, if $|F| = \theta$, then take $n = \mathcal{N}(F)$. Now,

$$\mathrm{rdu}(n) = |\mathcal{F}(\mathcal{N}(F))| = |F| = \theta.$$ □

It may feel at this point that we have saddled the reader with a great deal of notation without having accomplished much, given that the true difficulty is finding all possible Sophie Germain factorizations. However, given the set of factorizations, the following proposition provides a nice principle for organizing the solutions to (2). It measures the failure of $\mathcal{F}$ to be injective, and it is the main reason we have defined $\mathcal{F}$ and $\mathcal{N}$. The proof amounts to a reflection upon the meaning of the conditions used to divide the definition of $\mathcal{F}$ into four cases.

Proposition 3.3. *Let F_i be a Sophie Germain factorization of type i. Then,*

$$\mathcal{F}^{-1}(F_1) = \mathcal{N}(F_1) \cdot \{\textit{divisors of } 24\},$$
$$\mathcal{F}^{-1}(F_2) = \mathcal{N}(F_2) \cdot \{\textit{divisors of } 3\},$$
$$\mathcal{F}^{-1}(F_3) = \mathcal{N}(F_3) \cdot \{\textit{divisors of } 8\},$$
$$\mathcal{F}^{-1}(F_4) = \mathcal{N}(F_4) \cdot \{1\}.$$

We will use the above proposition in the next section.

4. Examples

Thankfully, it is now time to more concretely investigate the possible proportions of diagonal units using the tools developed above. We begin with Chebolu's theorem [2012].

4A. ***Chebolu's 24 theorem.*** We include this example for completeness; certainly, the proofs given in [Chebolu 2012] are either more direct or more interesting, or both.

Theorem 4.1 (Chebolu). *The ring $\mathbb{Z}_n$ satisfies the diagonal property if and only if n is a divisor of* 24.

Proof. We seek all possible solutions to $\mathrm{rdu}(n) = 1$. Since the integer 1 has the unique (type 1) Sophie Germain factorization 1, the solution set is

$$\begin{aligned}\mathcal{N}(1) \cdot \{\text{divisors of } 24\} &= 1 \cdot \{\text{divisors of } 24\} \\ &= \{\text{divisors of } 24\}.\end{aligned}$$

by Proposition 3.3. □

4B. ***Proof of Theorem 1.1.*** It is straightforward to check that when p is a Sophie Germain prime, the listed sets provide solutions to $\mathrm{rdu}(n) = p$. We therefore turn our attention to the converse.

Let $p > 3$ be prime and suppose $\mathrm{rdu}(n) = p$ has a solution, in which case p admits a Sophie Germain factorization. Any such factorization F of p must have $s = t = 0$ and $r = 1$ since p cannot have more than one distinct prime factor. Hence, $|F| = \theta(2\theta+1)^\beta$. Further, since $\theta(2\theta+1)^\beta = p$ and $\theta > 1$, we must have $\theta = p$ and $\beta = 0$. Thus,

$$p \cdot (2p+1)^0$$

is the only possible Sophie Germain factorization of p. This forces $2p+1$ to be prime, so p is a Sophie Germain prime and the set of solutions to $\mathrm{rdu}(n) = p$ is

$$\mathcal{N}(p \cdot (2p+1)^0) \cdot \{\text{divisors of } 24\} = (2p+1) \cdot \{\text{divisors of } 24\}$$

by Proposition 3.3.

For $p = 2$, the only Sophie Germain factorizations of 2 are $2 \cdot 5^0$ and $2^1 \cdot 1$. The first factorization has type 1, and the second has type 2. Note that $\mathcal{N}(2 \cdot 5^0) = 5$ and $\mathcal{N}(2^1 \cdot 1) = 16$. Hence, the set of solutions to $\mathrm{rdu}(n) = 2$ is

$$5 \cdot \{\text{divisors of } 24\} \cup 16 \cdot \{\text{divisors of } 3\}.$$

Finally, for $p = 3$, we have the type 1 factorization $3 \cdot 7^0$ with $\mathcal{N} = 7$ and the type 3 factorization $3^1 \cdot 1$ with $\mathcal{N} = 9$. Hence, the set of solutions to $\mathrm{rdu}(n) = 3$ is

$$7 \cdot \{\text{divisors of } 24\} \cup 9 \cdot \{\text{divisors of } 8\}.$$

This completes the proof of Theorem 1.1.

4C. ***Prime power ratios.*** We now consider the more general case $\mathrm{rdu}(n) = p^k$ for $k \geq 1$. First, assume $p > 3$ is prime.

Any Sophie Germain factorization of p^k must have the property that $s = t = 0$ and each θ_i is a positive power of p. Since p cannot divide both θ_i and $2\theta_i + 1$, we must have $\beta_i = 0$ for all i. Thus, every Sophie Germain factorization must have the form

$$\prod_{i=1}^{r} p^{k_i}(2p^{k_i} + 1)^0,$$

where the integers $2p^{k_1} + 1, \ldots, 2p^{k_r} + 1$ are distinct primes and $\sum k_i = k$ is a partition of k into distinct odd parts (each k_i is odd because $2p^v + 1$ is divisible by 3 whenever v is even). Each such factorization contributes

$$\prod_{i=1}^{r}(2p^{k_i} + 1) \cdot \{\text{divisors of } 24\}$$

to the set of solutions to $\mathrm{rdu}(n) = p^k$. Here are several examples of what may be gleaned from this discussion:

(A) There is no solution to $\mathrm{rdu}(n) = p^k$ when $p \equiv 1 \pmod 3$ (since this implies that $2p^v + 1$ is always divisible by 3).

(B) There is no solution to $\mathrm{rdu}(n) = p^2$ since there is no partition of 2 into distinct odd parts.

(C) There is a solution to $\mathrm{rdu}(n) = p^4$ if and only if $2p+1$ and $2p^3+1$ are both prime.

(D) There is a solution to $\mathrm{rdu}(n) = p^7$ if and only if $2p^7 + 1$ is prime.

(E) There is a solution to $\mathrm{rdu}(n) = p^8$ if and only if either $\{2p + 1, 2p^7 + 1\}$ or $\{2p^3 + 1, 2p^5 + 1\}$ is a set of primes.

The prime $p = 5$ illustrates (C). The prime $p = 677$, which is not a Sophie Germain prime, illustrates (D). For (E), $p = 29$ is a prime where both of the indicated sets are sets of primes; $p = 149$ is a prime where the second set is a set of primes and neither element of the first set is prime; $p = 179$ is a prime where the first set is a set of primes and neither element of the second set is prime.

The situations for the primes 2 and 3 are similar, so will only discuss the case $p = 2$. A Sophie Germain factorization of 2^k must be of type 1 or 2. For type 1 factorizations, one obtains solutions as above: k must admit a partition into distinct positive integers such that $2 \cdot 2^{k_i} + 1 = 2^{k_i+1} + 1$ is prime. Such primes are called Fermat primes, and $k_i + 1$ is forced to be a power of 2, so again each k_i must be odd. It is unknown whether there are infinitely many Fermat primes, therefore it is unknown whether there are infinitely many powers of 2 such that $\mathrm{rdu}(n) = 2^k$ admits a type 1 solution. A type 2 factorization must take the form $2^s \cdot \theta$, where θ is

a type 1 Sophie Germain factorization of 2^{k-s}. Since 3 is a Fermat prime, and the set of all solutions is obtained by multiplying the relevant $\mathcal{N}$-values by divisors of 3 or 24, we obtain that $\mathrm{rdu}(n)$ is a power of 2 if and only if $n = 2^s p_1 \cdots p_t$, where $s \geq 0$ and $p_1, \ldots, p_t$ is a (possibly empty) list of distinct Fermat primes.

This provides an interesting connection between the ratio of diagonal units and a classical result of Gauss and Wantzel (see [Pollack 2009]): it is possible to construct a regular n-sided polygon in the plane with straightedge and compass if and only if n takes the form given at the end of the previous paragraph. Gauss proved that the condition on n is necessary, and Wantzel proved that it is sufficient. Gauss' decision to devote his life to mathematics was in part due to his discovery at age 18 of the constructibility of the regular 17-gon. We summarize our observation in the next theorem.

Theorem 4.2. *Let n be a positive integer. The following statements are equivalent.*

(A) *The ratio of diagonal units in $\mathbb{Z}_n$ is a power of 2.*

(B) *The integer n has the form $2^s p_1 \cdots p_t$, where $s \geq 0$ and $p_1, \ldots, p_t$ is a (possibly empty) list of distinct Fermat primes.*

(C) *It is possible to construct a regular n-gon in the plane with straightedge and compass.*

The authors wish to thank Sunil Chebolu for noticing this connection to the Gauss–Wantzel theorem.

4D. ***Pairs of distinct primes.*** Call a positive integer n a *Sophie Germain number* if $2n+1$ is prime. In all of the cases thus far considered, the integer θ is a product of Sophie Germain numbers whenever $\mathrm{rdu}(n) = \theta$ has a solution. We include this section mainly to give a family of simple examples where this is not necessarily the case.

Let $3 < p < q$ be distinct primes. The possible Sophie Germain factorizations of pq are $p(2p+1)^0 q(2q+1)^0$ (if p and q are each Sophie Germain primes), $(pq)(2pq+1)^0$ (if pq is a Sophie Germain number), and $p \cdot q^0$ (if p is a Sophie Germain prime with safe prime $q = 2p+1$). Each of these factorizations is type 1, so the solution sets (provided they exist) are $(2p+1) \cdot \{\text{divisors of } 24\}$, $(2p+1)(2q+1) \cdot \{\text{divisors of } 24\}$, and $(2p+1)^2 \cdot \{\text{divisors of } 24\}$, respectively.

The integer $1081 = 23 \cdot 47$ is not expressible as a product of Sophie Germain numbers since, though $2 \cdot 23 + 1 = 47$ is prime, neither $2 \cdot 47 + 1 = 95$ nor $2 \cdot 23 \cdot 47 + 1 = 2163$ is prime. However, $\mathrm{rdu}(n) = 1081$ has solution set

$$47^2 \cdot \{\text{divisors of } 24\}.$$

4E. ***Further questions.*** We conclude this section with a few questions to ponder.

- The set of primes such that $\mathrm{rdu}(n) = p$ has a solution is precisely the set of Sophie Germain primes. From (B) in Section 4C we see that the set of primes

such that $\mathrm{rdu}(n) = p^2$ has a solution is the set $\{2, 3\}$ (since $\mathrm{rdu}(2^5) = 2^2$ and $\mathrm{rdu}(3^3) = 3^2$). For $k > 2$, what can we say about the set of primes such that $\mathrm{rdu}(n) = p^k$ has a solution? Is it always nonempty? When is it finite?

- If $p \equiv 2 \pmod 3$, must $\mathrm{rdu}(n) = p^k$ have a solution for some k?
- The number of partitions of k into distinct odd parts is the same as $s(k)$, the number of self-conjugate partitions of k. The maximum number of solutions to $\mathrm{rdu}(n) = p^k$ (for $p > 3$ prime) is $8 \cdot s(k)$. For each k, how many primes actually achieve this maximum value?
- Let k be a positive integer. Call a prime p a k-Sophie Germain prime (k-SGP) if k admits a partition into distinct odd parts and $2p^{k_1} + 1, \ldots, 2p^{k_r} + 1$ is a list of prime numbers for every partition $k = k_1 + \cdots + k_r$ of k into distinct odd parts. The value $k = 1$ corresponds to an ordinary Sophie Germain prime, and there are no 2-SGPs. A prime p is a 3-SGP if and only if $2p^3 + 1$ is prime; a prime p is an 8-SGP if and only if $2p + 1, 2p^7 + 1, 2p^3 + 1$, and $2p^5 + 1$ are prime. Does a k-SGP exist for each $k > 2$?

5. The multiplication cube for $\mathbb{Z}_n$

One could also analyze the multiplication cube for $\mathbb{Z}_n$. We know 1s lie exclusively on the diagonal if and only if $n = 1$ or 2 since otherwise $(-1) \cdot (-1) \cdot 1$ gives a 1 off the diagonal. Since this question seems uninteresting, we might require that every 1 in the multiplication table that is not in a coordinate plane (where one entry in the product is equal to 1) lies on the diagonal. The number of 1s appearing in the multiplication cube for $\mathbb{Z}_n$ is $\phi(n)^2$. (The first and second coordinates may be completely arbitrary units, but then the third coordinate is determined.) The number of 1s off all coordinate planes is $\phi(n)^2 - 3\phi(n) + 3 - 1$ (by the principle of inclusion/exclusion), and we wish to find values of n where this quantity is equal to the number of elements of multiplicative order precisely 3 (since the entry for $1 \cdot 1 \cdot 1$ has been omitted). Put another way, we wish to find values of n such that $\phi(n)^2 - 3\phi(n) + 3$ is equal to the number of elements of order dividing 3. In $\mathbb{Z}^\times_{p^k}$ there is one element of order dividing 3 if $p \equiv 2\,(3)$; three such elements if $p \equiv 1\,(3)$; one such element if $p = 3$ and $k = 1$; and three such elements if $p = 3$ and $k \geq 2$. Hence, the number of elements of $\mathbb{Z}^\times_n$ whose order divides 3 is $3^{r+\epsilon}$, where r is the number of prime divisors congruent to 1 modulo 3 and $\epsilon = 1$ if 9 divides n and $\epsilon = 0$ otherwise. We must now consider the equation $\phi(n)^2 - 3\phi(n) + 3 = 3^{r+\epsilon}$. If 3 divides the right-hand side, then 3 divides $\phi(n)^2$, so in fact 9 divides $\phi(n)^2 - 3\phi(n)$. This means 9 cannot divide the right-hand side, so we need only consider $\phi(n)^2 - 3\phi(n) + 3 = 1$ or 3. This in turn forces $\phi(n) = 1$ or 2 ($\phi(n)$ cannot equal 3). The only values of n satisfying either of these equalities are $n = 1, 2, 3, 4$, and 6. Conversely, it is easy to check that for $n = 1, 2, 3, 4$ or 6,

all 1s in the multiplication cube lie on the diagonal or the coordinate planes. This proves the following theorem.

Theorem 5.1. *All* 1*s in the multiplication cube for* $\mathbb{Z}_n$ *lie exclusively on the diagonal or the coordinate planes* (*where one of the three coordinates is* 1) *if and only if* n *is a divisor of* 4 *or* 6.

References

[Burton 1989] D. M. Burton, *Elementary number theory*, 2nd ed., W. C. Brown, Dubuque, IA, 1989. MR 90e:11001 Zbl 0696.10002

[Chebolu 2012] S. K. Chebolu, "What is special about the divisors of 24?", *Math. Mag.* **85**:5 (2012), 366–372. Zbl 1274.97016

[Cohen 2007] H. Cohen, *Number theory, I: Tools and Diophantine equations*, Graduate Texts in Mathematics **239**, Springer, New York, 2007. MR 2008e:11001 Zbl 1119.11001

[Laubenbacher and Pengelley 1999] R. Laubenbacher and D. Pengelley, *Mathematical expeditions: Chronicles by the explorers*, Springer, New York, 1999. MR 99i:01005 Zbl 0919.01001

[Pollack 2009] P. Pollack, *Not always buried deep: A second course in elementary number theory*, Amer. Math. Soc., Providence, RI, 2009. MR 2010i:11003 Zbl 1187.11001

Received: 2014-06-09 Revised: 2014-06-09 Accepted: 2014-07-15

genzka01@alumni.gettysburg.edu *Department of Mathematics, Gettysburg College, Gettysburg, PA 17325, United States*

klockrid@gettysburg.edu *Department of Mathematics, Gettysburg College, Gettysburg, PA 17325, United States*

involve

msp.org/involve

See inside back cover or msp.org/involve for submission instructions. The subscription price for 2015 is US $140/year for the electronic version, and $190/year (+$35, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to MSP.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840, is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFlow® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

involve
2015 vol. 8 no. 4