When do the Curves $xy \equiv 1 \pmod{n}$ and $x^2 + y^2 \equiv 1 \pmod{n}$ Intersect?

Sara Hanrahan and Mizan R. Khan

The second author, MK, would like to dedicate this note to his brother Riaz for introducing him (MK) to the joys of doing elementary mathematics!

Introduction

The figure below illustrates the simple fact that the hyperbola $xy = 1$ does not intersect the unit circle $x^2 + y^2 = 1$ in $\mathbb{R}^2$.

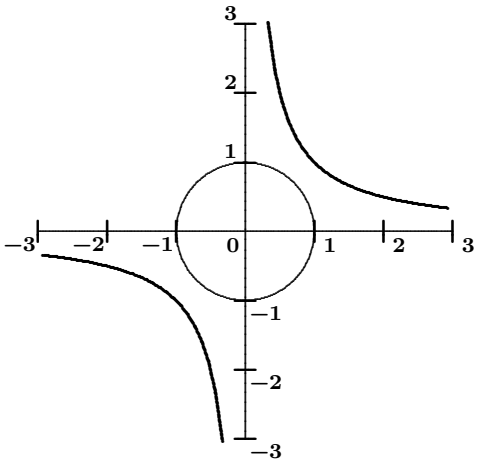

Figure 1. The curves $xy = 1$ and $x^2 + y^2 = 1$

In the course of some investigations in modular arithmetic, we asked ourselves the question of whether the unit modular circle

$$\mathcal{C}_n = \{(x, y) : x, y \in \mathbb{Z}_n \text{ and } x^2 + y^2 \equiv 1 \pmod{n}\}$$

could intersect the modular hyperbola

$$\mathcal{H}_n = \{(x, y) : x, y \in \mathbb{Z}_n \text{ and } xy \equiv 1 \pmod{n}\}.$$

For example, $\mathcal{C}_{17} \cap \mathcal{H}_{17} = \emptyset$, but $\mathcal{C}_{37} \cap \mathcal{H}_{37} \neq \emptyset$, a fact illustrated in the figures on the next page. Note that in our graphs of $\mathcal{C}_n$ and $\mathcal{H}_n$ we introduce the restriction that $0 \leq x, y \leq n - 1$.

Crux Mathematicorum with Mathematical Mayhem, Volume 37, Issue 6

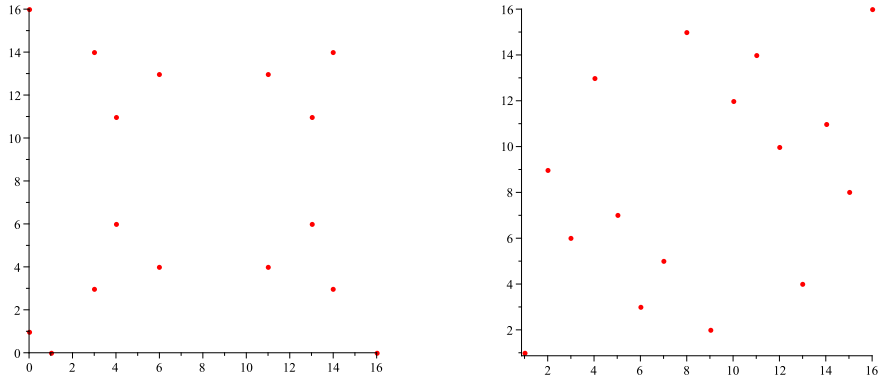

Figure 2. The curves $\mathcal{C}_{17}$ and $\mathcal{H}_{17}$

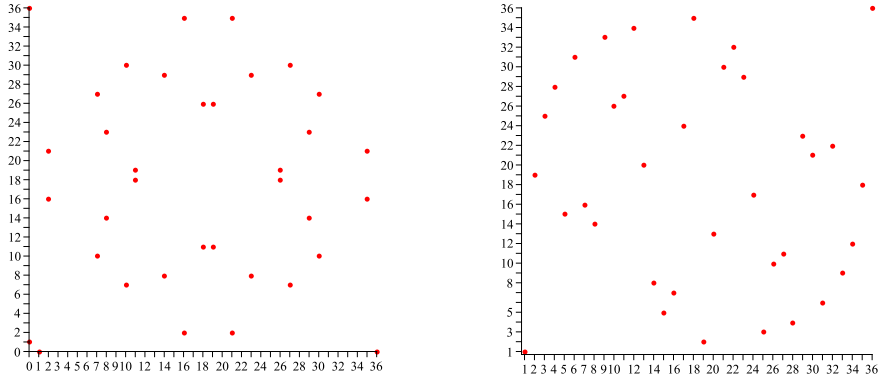

Figure 3. The curves $\mathcal{C}_{37}$ and $\mathcal{H}_{37}$

A more striking visual example of when the curves don't intersect is $n = 787$:

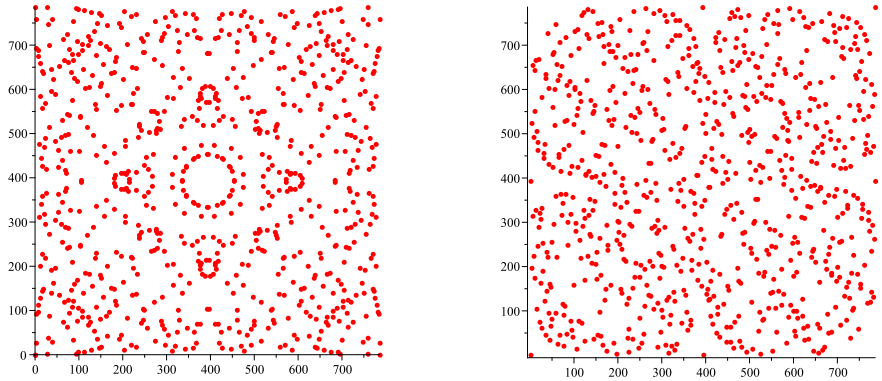

Figure 4. The curves $\mathcal{C}_{787}$ and $\mathcal{H}_{787}$

Eventually we discovered a neat little result about the prime factorization of integers n for which $\mathcal{C}_n \cap \mathcal{H}_n \neq \emptyset$. Specifically, we have the following result.

Theorem 1 It is the case that $\mathcal{C}_n \cap \mathcal{H}_n \neq \emptyset$ if and only if every prime in the canonical factorization of n is congruent to 1 modulo 12.

Background Material

We will prove Theorem 1 by using three basic results in number theory: the Chinese Remainder Theorem, the Law of Quadratic Reciprocity, and a special case of Hensel's lemma. We now give short descriptions of each of these results and refer the reader to [1] for the detailed proofs.

The Chinese Remainder Theorem

The Chinese Remainder Theorem addresses the following type of problem. Is there a positive integer x which when divided by 107 leaves a remainder of 60 and when divided by 256 leaves a remainder of 38? Alternatively, in the language of congruences, can we simultaneously solve

$$x \equiv 60 \pmod{107} \qquad \text{and} \qquad x \equiv 38 \pmod{256} \ ?$$

The Chinese Remainder Theorem says that if the moduli 107 and 256 are relatively prime (which they are), then the answer is yes. The surprise is that the numbers 60 and 38 play no role — only the relationship between 107 and 256 matters.

Theorem 2 (Chinese Remainder Theorem) Let $m_1, m_2, \ldots, m_k$ be integers such that $\gcd(m_i, m_j) = 1$ whenever $i \neq j$, and let $a_1, a_2, \ldots, a_k$ be arbitrary integers. Then the congruences

$$x \equiv a_i \pmod{m_i} \ , \quad i = 1, 2, \ldots, k$$

have a common solution, and any two solutions are congruent modulo the product $m = m_1 m_2 \cdots m_k$.

A brief sketch of the proof runs as follows. Let $n_i = m/m_i$. Clearly, $\gcd(n_1, n_2, \ldots, n_k) = 1$. Therefore, by the Extended Euclidean Algorithm, there are integers s_i such that

$$s_1 n_1 + s_2 n_2 + \cdots + s_k n_k \ = \ 1 \, .$$

We now take

$$x \ = \ a_1 s_1 n_1 + a_2 s_2 n_2 + \cdots + a_k s_k n_k \, .$$

(See [1], Theorem 3.10, page 53 for more details.)

The Law of Quadratic Reciprocity

The Law of Quadratic Reciprocity deals with questions of when elements of $\mathbb{Z}_n$ have square roots. For example, does the congruence $x^2 \equiv 12 \pmod{97}$ have a solution? The Law of Quadratic Reciprocity provides a very simple relationship when we are working with primes. We first introduce some terminology and the Legendre symbol $(\cdot/p)$. Let p be a prime and a an integer such that $\gcd(a,p) = 1$. We say that a is a *quadratic residue* modulo p if the congruence

$$x^2 \equiv a \pmod{p}$$

has a solution. If this congruence has no solution, then we say that a is a *quadratic nonresidue* modulo p. The Legendre (a/p) is a convenient way to denote whether or not a is a residue or nonresidue modulo p.

Definition For p a prime and a an integer we define the Legendre symbol (a/p) as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } \gcd(a,p) = 1 \text{ and } a \text{ is a quadratic residue mod } p\,, \\ -1, & \text{if } \gcd(a,p) = 1 \text{ and } a \text{ is a quadratic nonresidue mod } p\,, \\ 0, & \text{if } p|a\,. \end{cases}$$

From here on p will always denote an *odd* prime. From the fact that the multiplicative group $\mathbb{Z}_p^*$ is cyclic we can prove that

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}\,,$$

and consequently -1 has a square root in $\mathbb{Z}_p$ if and only if $p \equiv 1 \pmod{4}$. However, for other numbers this is a more difficult question to answer. For example, when is 3 a square root modulo p? An eminently satisfactory answer to such questions is given by the Law of Quadratic Reciprocity.

Theorem 3 (Law of Quadratic Reciprocity) Let p and q be two distinct odd primes. Then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}\,.$$

Euler and Lagrange were the first to formulate this law, but Gauss gave the first proof in his masterpiece *Disquisitiones Arithmeticae*. This was Gauss' favourite theorem and in his lifetime he gave eight different proofs. There are a great many proofs of the Law of Quadratic Reciprocity ranging from elementary to highly sophisticated, but none are straightforward. An elementary and understandable proof is given in [1], pages 133–135.

Using this law one can answer our earlier question of when 3 is a square root modulo p: it is when $p \equiv \pm 1 \pmod{12}$ — a key fact that we will use in our proof of Theorem 1. For completeness we give a proof as follows.

Proof. Let $p \geq 5$. Combining the Law of Quadratic Reciprocity with the observation that if $\gcd(a,p) = 1$ then $(a/p)^2 = 1$, we get

$$\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{3}\right).$$

Therefore, $(3/p) = 1$ if and only if we have one of the following two conditions: (1) $\frac{p-1}{2}$ is even and p is a quadratic residue modulo 3; or (2) $\frac{p-1}{2}$ is odd and p is a quadratic nonresidue modulo 3.

Condition 1 is equivalent to the two congruences $p \equiv 1 \pmod 4$ and $p \equiv 1 \pmod 3$. By the Chinese Remainder Theorem this is equivalent to the single congruence $p \equiv 1 \pmod{12}$. Condition 2 is equivalent to the two congruences $p \equiv 3 \pmod 4$ and $p \equiv 2 \pmod 3$. By the Chinese Remainder Theorem this is equivalent to the single congruence $p \equiv 11 \pmod{12}$. Thus,

$$\left(\frac{3}{p}\right) = 1 \iff p \equiv \pm 1 \pmod{12}.$$

Hensel's lemma

Hensel's lemma answers the following type of problem. Suppose we are told that the congruence $x^2 \equiv 28 \pmod{37}$ has the solutions $x = 18$ and $x = 19$. What does this piece of information tell us about the existence of solutions to the congruence

$$x^2 \equiv 28 \pmod{37^3}\ ?$$

Hensel's lemma gives an affirmative answer to this question.

Theorem 4 (Hensel's lemma, quadratic version) Let a be a quadratic residue modulo p. Then the congruence

$$x^2 \equiv a \pmod{p^k}$$

has a solution for all $k \geq 1$.

The basic idea of the proof is to start with a solution of $x^2 \equiv a \pmod p$ and "lift" it to $x^2 \equiv a \pmod{p^2}$ and repeat. This process is particularly straightforward for such quadratic congruences. For more general polynomial congruences $f(x) \equiv a \pmod{p^n}$, one needs the hypothesis that the solution is not a zero of the derivative $f'(x)$. See [1], Sections 4.3 and 7.5 for more details.

Finally, the way one solves quadratic congruences $x^2 \equiv a \pmod n$ for composite n is to first solve it for each prime divisor of n, and then combine Hensel's lemma with the Chinese Remainder Theorem to find a solution.

The Proof of Theorem 1

Suppose that $\mathcal{C}_n \cap \mathcal{H}_n \neq \emptyset$. Then $\mathcal{C}_p \cap \mathcal{H}_p \neq \emptyset$ for any prime divisor p of n. It is easy to check that both intersections $\mathcal{C}_2 \cap \mathcal{H}_2$ and $\mathcal{C}_3 \cap \mathcal{H}_3$ are empty, and consequently $p \geq 5$. We now prove that $p \equiv 1 \pmod{12}$. Let $(r, s) \in \mathcal{C}_p \cap \mathcal{H}_p$. We have

$$\begin{aligned} (r-s)^2 &\equiv -1 \pmod{p} , \\ (r+s)^2 &\equiv 3 \pmod{p} , \end{aligned}$$

that is, $(-1/p) = (3/p) = 1$, where $(\cdot/p)$ is the Legendre symbol. Since

$$\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \pmod{4}$$

and

$$\left(\frac{3}{p}\right) = 1 \iff p \equiv \pm 1 \pmod{12} ,$$

we conclude that $p \equiv 1 \pmod{12}$.

Conversely let $n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ be the canonical factorization of n and suppose $p_i \equiv 1 \pmod{12}$ for each i. We will show that $\mathcal{C}_n \cap \mathcal{H}_n \neq \emptyset$.

For each i both -1 and 3 are squares modulo p_i, since $p_i \equiv 1 \pmod{12}$. Using Theorem 4 we lift these square roots to the $e_i{}^{\text{th}}$ power, $p_i^{e_i}$. Let s_i and r_i be such that $s_i^2 \equiv -1 \pmod{p_i^{e_i}}$, and $r_i^2 \equiv 3 \pmod{p_i^{e_i}}$. Then

$$2^{-1} \cdot (r_i + s_i, r_i - s_i) \in \mathcal{C}_{p_i^{e_i}} \cap \mathcal{H}_{p_i^{e_i}} ,$$

where 2^{-1} denotes the inverse of 2 modulo $p_i^{e_i}$. We now invoke the Chinese Remainder Theorem to determine integers r and s such that

$$\begin{aligned} r &\equiv r_i \pmod{p_i^{e_i}} , \\ s &\equiv s_i \pmod{p_i^{e_i}} , \end{aligned}$$

for each $i = 1, 2, \ldots, t$. Clearly, $2^{-1} \cdot (r+s, r-s) \in \mathcal{C}_n \cap \mathcal{H}_n$, and the proof is complete.

References

[1] G.A. Jones and J.M. Jones, *Elementary Number Theory*, Springer-Verlag, 1998.

Sara Hanrahan Mizan R. Khan
Dept. of Mathematics and Computer Science
Eastern Connecticut State University
Willimantic, CT 06226
USA
hanrahans@stu.easternct.edu khanm@easternct.edu