Week 10

15.2 Non-Terminating Decimal expansions

Among the expansions in Table 15.1 that do not terminate are some with long periods, e.g. 17, 19, 23, 29. In each case n is a prime and the period of $1/n$ is $n-1$. But not all primes p have $p-1$ as the period of the expansion of $1/p$. For example, $1/3$ has period 1, not 2, $1/13$ has period 6, not 12, $1/11$ has period 2, not 10... does this ring a bell?

The following theorem is a first step in determining the length of the periods of reciprocals.

★ Note that the proof in Dudley contains several errors – he does not even prove what he sets out to prove. Use the proof below instead. (Omitted in class because this result is a corollary to other theorems we will prove.)

Theorem 15.3 *The length of the decimal period of* $1/n$ *is at most* $n-1$.

Proof. If $n = 2^a 5^b$ for some nonnegative integers a and b, then the decimal expansion terminates, so we may assume that $n \neq 2^a 5^b$; in particular, $n \neq 10^k$ for any nonnegative integer k. Let t be the (unique) integer such that

$$10^t < n < 10^{t+1}.$$

Using the division algorithm, we have

$$\begin{aligned}
10^{t+1} &= d_1 n + r_1, && 0 < r_1 < n, && (15.2)\\
10r_1 &= d_2 n + r_2, && 0 \le r_2 < n,\\
10r_2 &= d_3 n + r_3, && 0 \le r_3 < n,\\
&\vdots\\
10r_{k-1} &= d_k n + r_k, && 0 \le r_{k+1} < n,\\
10r_k &= d_{k+1} n + r_{k+1}, && 0 \le r_{k+1} < n, && (15.3)\\
&\vdots
\end{aligned}$$

and so on.

- Note that $d_k < 10$ for each k, because for $k = 2, 3, ...,$

$$d_k n = 10r_{k-1} - r_k \le 10r_{k-1} < 10n,$$

and for $k = 1$,

$$d_1 n = 10^{t+1} - r_1 < 10^{t+1} = 10 \cdot 10^t < 10n.$$

If we divide both sides of (15.3) by $10n$, we get

$$r_k/n = d_{k+1}/10 + r_{k+1}/10n. \tag{15.4}$$

If we divide both sides of (15.2) by $10^{t+1}n$ and apply (15.4) repeatedly, we get

$$\begin{aligned} 1/n &= d_1/10^{t+1} + r_1/n \cdot 10^{t+1} \\ &= d_1/10^{t+1} + d_2/10^{t+2} + r_2/n \cdot 10^{t+2} \\ &= d_1/10^{t+1} + d_2/10^{t+2} + d_3/10^{t+3} + r_3/n \cdot 10^{t+3} \\ &\vdots \\ &= d_1/10^{t+1} + d_2/10^{t+2} + d_3/10^{t+3} + d_4/10^{t+4} + \cdots . \end{aligned} \tag{15.5}$$

Thus $d_1, d_2, d_3, ...$ are the digits of the decimal expansion of $1/n$.

- If the remainder $r_k = 0$ for some k, then (15.5) becomes

  $$1/n = d_1/10^{t+1} + d_2/10^{t+2} + \cdots + d_k/10^{t+k}$$

  and so the decimal expansion of $1/n$ terminates, which, by assumption, it does not. Hence $r_k \neq 0$ for all k.

Therefore each of $r_1, r_2, ...$ has one of the $n-1$ values $1, 2, ..., n-1$. Hence by the pigeonhole principle, among the n integers $r_1, r_2, ..., r_n$ there are two that are equal. Say $r_j = r_k$ for some j and k with $k < j$. Then from the equations (15.2) to (15.3), $d_{j+1} = d_{k+1}$, $d_{j+2} = d_{k+2}$, ..., and the decimal repeats with period no greater than $n-1$. ■

If n is relatively prime to 10, we know more about the period of $1/n$.

★ Note that Dudley now completely forgets that he has written Section 10 on primitive roots. We give a different formulation of Theorem 15.4.

Theorem 15.4 *If* $(10, n) = 1$*, then the period of the decimal expansion of* $1/n$ *is the order of* $10 \pmod{n}$.

Proof. Note that $\operatorname{ord}_n 10$ is defined because $(10, n) = 1$. Let $r = \operatorname{ord}_n 10$. Then $10^r \equiv 1 \pmod{n}$ and hence

$$10^r - 1 = kn \tag{15.6}$$

for some integer k. Obviously, $k < 10^r$ and so we may write

$$\begin{aligned} k &= d_{r-1}10^{r-1} + d_{r-2}10^{r-2} + \cdots + d_1 10 + d_0 \\ &= d_{r-1}d_{r-2}...d_1d_0 \quad \text{(digital representation)}, \end{aligned}$$

where $0 \le d_k < 10$ for each $k = 0, 1, ..., r-1$. Then from (15.6),

$$\begin{aligned}
\frac{1}{n} &= \frac{k}{10^r - 1} = \frac{k}{10^r(1 - 10^{-r})} \\
&= \frac{d_{r-1}d_{r-2}...d_1d_0}{10^r} \cdot \frac{1}{1 - 10^{-r}} \\
&= (.d_{r-1}d_{r-2}...d_1d_0)(1 + 10^{-r} + 10^{-2r} + \cdots) \\
&= (.d_{r-1}d_{r-2}...d_1d_0) + (.\underbrace{00...0}_{r\ 0\text{s}}d_{r-1}d_{r-2}...d_1d_0) + (.\underbrace{00...0}_{2r\ 0\text{s}}d_{r-1}d_{r-2}...d_1d_0) + \cdots \\
&= (.\overline{d_{r-1}d_{r-2}...d_1d_0}).
\end{aligned}$$

Thus the period of $1/n$ is at most r.

We now show that the period is no less than r.
Suppose the period of $1/n$ is s, that is,

$$\frac{1}{n} = (.\overline{e_{s-1}e_{s-2}...e_1e_0})$$

for some integers $e_0, e_1, ..., e_{s-1}$, $0 \le e_i < 10$. Then (by definition of the period of the expansion) $s \le r$. Also,

$$\begin{aligned}
\frac{1}{n} &= (.e_{s-1}e_{s-2}...e_1e_0)(1 + 10^{-s} + 10^{-2s} + \cdots) \\
&= \frac{e_{s-1}e_{s-2}...e_1e_0}{10^s} \cdot \frac{1}{1 - 10^{-s}} \\
&= \frac{e_{s-1}e_{s-2}...e_1e_0}{10^s - 1}.
\end{aligned}$$

But then $n(e_{s-1}e_{s-2}...e_1e_0) = 10^s - 1$, thus $n|(10^s - 1)$, which means that $10^s \equiv 1 \pmod{n}$. Since $r = \text{ord}_n\, 10$, it follows that $s \ge r$ and so $r = s$. ■

- Hence if $(10, n) = 1$, then the period of the decimal expansion of $1/n$ is $n - 1$ if and only if n is prime and 10 is a primitive root of n.

Theorem 15.4 can be generalized to find the period of the expansion of $1/n$ in any base b, where $(b, n) = 1$.

Theorem 15.4A. *If $(b, n) = 1$, then the period of the expansion of $1/n$ in base b is the order of $b \pmod{n}$.* (See Problem 8.)

Example: Determine the period of the decimal expansion of 1/33. Then determine the decimal expansion of 1/33.

Solution

Since $(10, 33) = 1$, the period of the expansion of $1/33$ is $\text{ord}_{33}\, 10$. Note that $\phi(33) = \phi(3)\phi(11) = 2 \cdot 10 = 20$, so $\text{ord}_{33}\, 10 | 20$. But

$$10^2 \equiv 100 \equiv 3 \cdot 33 + 1 \equiv 1 \pmod{33}.$$

Thus $\text{ord}_{33}\, 10 = 2$.

We determine $1/33$ in the following way to illustrate the method we have to use for expansions in other bases. Write $99 = 10^2 - 1$ as $99 = 33k$, where k has $2 = \text{ord}_{33}\, 10$ digits (to keep track of decimal places). Thus $k = 03$. Now $1/33 = 0.\overline{03}$, because

$$\begin{aligned}\frac{1}{33} = \frac{k}{10^2 - 1} = \frac{03}{10^2 - 1} = \frac{03}{10^2(1 - 10^{-2})} = \frac{03}{10^2} \cdot \frac{1}{1 - 10^{-2}} \\ = 0.03(1 + 10^{-2} + 10^{-4} + \cdots) \\ = 0.\overline{03}.\end{aligned}$$

15.3 Expansions in Other Bases

Example: Determine the period of the expansion of $1/25$ in base 6. Then determine the expansion of $1/25$ in base 6.

Solution

Since $(6, 25) = 1$, the period is $t = \text{ord}_{25}\, 6$. Since $\phi(25) = \phi(5^2) = 5 \cdot 4 = 20$, we know that $t | 20$.

$$\begin{aligned}6^2 &\equiv 36 \equiv 11 \pmod{25} \\ 6^4 &\equiv 11^2 \equiv 121 \equiv 21 \pmod{25} \\ 6^5 &\equiv 21 \cdot 6 \equiv 126 \equiv 1 \pmod{25}.\end{aligned}$$

Thus $t = 5$.

Now $6^5 \equiv 1 \pmod{25}$ implies that 25 divides $6^5 - 1 = 7775$; write 7775 as $7775 = 25k$, where $k = 311$. We must write 311 in base 6, using $t = 5$ place values.

$$\begin{aligned}311 &= 51 \cdot 6 + 5 \\ &= (8 \cdot 6 + 3) \cdot 6 + 5 = 8 \cdot 6^2 + 3 \cdot 6 + 5 \\ &= (1 \cdot 6 + 2) \cdot 6^2 + 3 \cdot 6 + 5 = 1 \cdot 6^3 + 2 \cdot 6^2 + 3 \cdot 6 + 5 \\ &= 0 \cdot 6^4 + 1 \cdot 6^3 + 2 \cdot 6^2 + 3 \cdot 6 + 5.\end{aligned}$$

Now $1/25 = (.\overline{01235})_6$, because from $6^5 - 1 = 25k$ and $6^5 - 1 = 6^5(1 - 6^{-5})$ we get

$$\begin{aligned}\frac{1}{25} = \frac{k}{6^5-1} &= \left(\frac{0\cdot 6^4 + 1\cdot 6^3 + 2\cdot 6^2 + 3\cdot 6 + 5}{6^5}\right)\left(\frac{1}{1-6^{-5}}\right)\\ &= \left(\frac{0}{6} + \frac{1}{6^2} + \frac{2}{6^3} + \frac{3}{6^4} + \frac{5}{6^5}\right)\left(\frac{1}{1-6^{-5}}\right)\\ &= (.01235)_6(1 + 6^{-5} + 6^{-10} + \cdots)\\ &= (.\overline{01235})_6\end{aligned}$$

Theorem 15.4 can also be generalized to find the period of the decimal expansion of any fraction whose expansion does not terminate. First write the fraction in lowest form, that is, in the form c/n where $(c, n) = 1$. If $n = 2^a5^b$, then the expansion terminates. If $n \neq 2^a5^b$, then write n in the form $n = 2^a5^bn_1$, where $n_1 > 1$ and $(10, n_1) = 1$.

Theorem 15.5 *If $n = 2^a5^bn_1$, where $n_1 > 1$, $(10, n_1) = 1$, and $(c, n) = 1$, then the period of the decimal expansion of c/n is $\operatorname{ord}_{n_1} 10$. The length of the non-periodical part of the expansion is M, where $M = \max\{a, b\}$.*

- Thus, with c/n in lowest form, where

$$n = 2^a5^bn_1,\ a, b \geq 0,\ \text{with } n_1 > 1 \text{ and } (10, n_1) = 1,$$

  the decimal period of c/n has length t, where $t|\phi(n_1)$, thus length at most $n_1 - 1$.

- It has length equal to $n_1 - 1$ if and only if $\phi(n_1) = n_1 - 1$, that is, n_1 is prime, and 10 is a primitive root of n_1.

- Hence the decimal period of c/n is $n - 1$ if and only if n is prime, $(10, n) = 1$ and 10 is a primitive root of n.

- As the length of the non-periodical part of the expansion is M, where $M = \max\{a, b\}$, the decimal expansion of c/n is **purely periodical** (has no non-periodical part) if and only if $M = 0$, that is, if and only if $(10, n) = 1$.

Example: Given that the least residue of 10 is a primitive root of 7, determine, with reasons, the period and the length of the non-periodical part of the decimal expansion of 18/2800.

Solution

Note that $18 = 2\times 3^2$ and $2800 = 2^45^27$. Thus in lowest form, $18/2800 = 9/2^35^27$. The length of the nonperiodical part of the expansion is $\max\{3, 2\} = 3$. The period of the expansion is $\operatorname{ord}_7 10$. Since the least residue of 10 is a primitive root of 7, $\operatorname{ord}_7 10 = 6$.

Here is how to find the expansion:

$$\frac{18}{2800} = \frac{9}{2^3 5^2 7} = \frac{9 \cdot 5}{2^3 5^3 7} = \frac{1}{10^3} \cdot \frac{45}{7} = \frac{1}{10^3}\left(6 + \frac{3}{7}\right) = \frac{6}{10^3} + \frac{1}{10^3} \cdot \frac{3}{7}.$$

Now, $10^6 \equiv 1 \pmod 7$, so $10^6 - 1 = 7k$ for some k. Find k and $3k$. Since $k = 142\,857$, $3k = 428571$. So

$$\begin{aligned}
\frac{9}{2^3 5^2 7} &= \frac{6}{10^3} + \frac{1}{10^3} \cdot \frac{3k}{10^6 - 1} \\
&= \frac{6}{10^3} + \frac{1}{10^3} \cdot \frac{428571}{10^6} \cdot (1 + 10^{-6} + 10^{-12} + \cdots) \\
&= 0.006 + \frac{1}{10^3}(.\overline{428571}) \\
&= 0.006 + 0.000\overline{428571} \\
&= 0.006\overline{428571}.
\end{aligned}$$

We can generalize Theorem 15.5 even further.

Consider the fraction c/n in lowest form and the integer b with prime-power decomposition $b = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$.

- If each prime factor of n is a prime factor p_i of b, then the expansion of c/n in base b terminates.
- If n has at least one prime factor other than those of b, write n as $n = p_1^{f_1} p_2^{f_2} \ldots p_k^{f_k} n_1$, where each $f_i \geq 0$, $n_1 > 1$ and $(b, n_1) = 1$. Then the period of the expansion in base b of c/n is $\operatorname{ord}_{n_1} b$.
- If $e_i = 1$ for each i, then the length of the non-periodical part is M, where $M = \max_{i=1}^{k}\{f_i\}$. (In general, the length of the non-periodical part is M, where M is the smallest integer such that $Me_i \geq f_i$ for all i, that is, M is the smallest integer such that $p_1^{f_1} p_2^{f_2} \ldots p_k^{f_k} | b^M$.)

  The expansion is purely periodical if and only if $(b, n) = 1$.

Section 16

Pythagorean Triangles

- A **Pythagorean triangle** is a right triangle whose sides are line segments whose lengths are denoted by integers.

The Babylonians of 3500 years ago knew from observation that triangles whose sides have integer lengths x, y and z with

$$x^2 + y^2 = z^2, \tag{16.1}$$

are right triangles, but it was only(!) 2500 years ago that the Pythagoreans proved that this is the case for all right triangles. The Babylonians could find some solutions to this equation; the aim in this section is to find them all. We may assume that $(x, y) = 1$, for if $(x, y) = d$, then $d|z$, and dividing both sides of (16.1) by d^2, we get

$$(x/d)^2 + (y/d)^2 = (z/d)^2,$$

where $(x/d, y/d) = 1$. Thus any solution of (16.1) can be derived from a solution in which the terms on the left are relatively prime, by multiplication with a suitable integer. Note that if $(x, y) = 1$ in (16.1), then $(x, z) = (y, z) = 1$.

16.1 Fundamental Pythagorean Triangles

- A solution of (16.1) of the form $x = a$, $y = b$, $z = c$ with $(a, b) = 1$ and a, b and c positive integers, is called a **fundamental solution**. Thus, in a fundamental solution,

$$(a, b) = (a, c) = (b, c) = 1. \tag{16.2}$$

A Pythagorean triangle whose side lengths satisfy (16.2) is called a **fundamental Pythagorean triangle**. We derive an expression for all fundamental solutions of (16.1) by proving four lemmas.

Lemma 16.1 *If a, b, c is a fundamental solution of* (16.1)*, then exactly one of a and b is even and so c is odd.*

Proof.
If $(a,b) = (a,c) = (b,c) = 1$, then a and b cannot both be even. Suppose a and b are both odd. Then $a \equiv 1$ or $3 \pmod 4$ and so $a^2 \equiv 1 \pmod 4$; similarly $b^2 \equiv 1 \pmod 4$. But then

$$c^2 \equiv a^2 + b^2 \equiv 1 + 1 \equiv 2 \pmod 4,$$

which is impossible because $c \equiv 0$ or $2 \pmod 4$ and so $c^2 \equiv 0 \pmod 4$. ■

Recall that if exactly one of a and b is even, we also say that a and b have **different parity**, or $a \not\equiv b \pmod 2$.

Lemma 16.2 *If $r^2 = st$ and $(s,t) = 1$, then both s and t are squares.*

Proof.
Suppose s and t have prime power decompositions

$$s = p_1^{e_1} p_2^{e_2} ... p_k^{e_k}$$
$$t = q_1^{f_1} q_2^{f_2} ... q_l^{f_l}.$$

Then the p_i are all distinct and the q_i are all distinct. Since $(s,t) = 1$, $p_i \neq q_j$ for all $i = 1, 2, ..., k$ and all $j = 1, 2, ..., l$. Thus r^2 has prime power decomposition $r^2 = p_1^{e_1} p_2^{e_2} ... p_k^{e_k} q_1^{f_1} q_2^{f_2} ... q_l^{f_l}$ in which all the primes are different. Since r^2 is a square, each e_i and f_j is even, from which it follows that s and t are squares. ■

Next we prove two lemmas.

Lemma 16.3 *Let a, b, c be a fundamental solution of (16.1), where a is even. Then there are positive integers m and n with $m > n$, $(m,n) = 1$ and $m \not\equiv n \pmod 2$, such that*

$$a = 2mn,$$
$$b = m^2 - n^2,$$
$$c = m^2 + n^2.$$

Proof.
Since a is even, $a = 2r$ for some r. Thus $a^2 = 4r^2$. But $a^2 + b^2 = c^2$, hence $a^2 = c^2 - b^2$ and so

$$4r^2 = (c+b)(c-b). \tag{16.3}$$

By Lemma 16.1, b and c are odd, so $c+b$ and $c-b$ are both even. Thus there are integers s and t such that

$$c + b = 2s \quad \text{and} \quad c - b = 2t, \tag{16.4}$$

that is,

$$c = s + t \quad \text{and} \quad b = s - t. \tag{16.5}$$

Substituting (16.4) into (16.3) and dividing by 4, we get

$$r^2 = st.$$

- If we can prove that s and t are both squares, say $s = m^2$ and $t = n^2$, then we will have $r^2 = m^2n^2$, thus $r = mn$, and so $a = 2r = 2mn$ as required. Moreover, from (16.5), b and c will be in the required form. So this is what we do next.

By Lemma 16.2, we only need to prove that $(s,t) = 1$. Suppose $d|s$ and $d|t$. Then by (16.5), $d|c$ and $d|b$. But by (16.2) above, $(b,c) = 1$ and so $d = 1$, that is, $(s,t) = 1$.

Thus let $s = m^2$ and $t = n^2$, where m and n are positive, so as explained above we now have

$$a = 2mn.$$

From (16.5),

$$c = s + t = m^2 + n^2,$$
$$b = s - t = m^2 - n^2.$$

To prove the lemma we must still prove that $m > n$, $(m,n) = 1$ and $m \not\equiv n \pmod 2$.

- ⋆ But a, b, c is a fundamental solution of (16.1), so $b > 0$, hence $m^2 > n^2$, and since m and n are positive, $m > n$.
- ⋆ Suppose $d|m$ and $d|n$. Then $d|s$ and $d|t$, so $d = 1$ since $(s,t) = 1$. Hence $(m,n) = 1$.
- ⋆ Since $(m,n) = 1$, m and n are not both even. Suppose m and n are both odd. Then s and t are both odd, and so by (16.5), b and c are both even, contradicting (16.2). ■

We also prove the converse of Lemma 16.3.

Lemma 16.4 *If m and n are integers such that*

$$\begin{aligned} a &= 2mn, \\ b &= m^2 - n^2, \\ c &= m^2 + n^2, \end{aligned}$$

then a, b, c is a solution of $x^2 + y^2 = z^2$. If in addition, $m > n$, m and n are positive, $(m, n) = 1$, and $m \not\equiv n \pmod 2$, then a, b, c is a fundamental solution.

Proof.
It is easy to see that a, b, c is a solution:

$$\begin{aligned} a^2 + b^2 &= (2mn)^2 + (m^2 - n^2)^2 \\ &= (m^2)^2 + (n^2)^2 - 2m^2n^2 + 4m^2n^2 \\ &= (m^2)^2 + (n^2)^2 + 2m^2n^2 \\ &= (m^2 + n^2)^2 \\ &= c^2. \end{aligned}$$

We next assume that $(m, n) = 1$ and $m \not\equiv n \pmod 2$, and show that $(a, b) = 1$.

Note that a is even. Since $m \not\equiv n \pmod 2$, exactly one of m and n is even, and so b is odd. Hence if a and b do have a common factor, then this factor is odd, hence is divisible by an odd prime.

So suppose, contrary to the statement $(a, b) = 1$, that p is an odd prime such that $p|a$ and $p|b$. Since $a^2 + b^2 = c^2$, it follows that $p|c$. From $p|b$ and $p|c$ we get $p|(b + c)$ and $p|(b - c)$. But

$$b + c = m^2 - n^2 + m^2 + n^2 = 2m^2$$

and

$$b - c = m^2 - n^2 - m^2 - n^2 = -2n^2.$$

Thus, since p is odd,

$$p|m^2 \quad \text{and} \quad p|n^2,$$

and since p is prime,

$$p|m \quad \text{and} \quad p|n.$$

However, $(m, n) = 1$, a contradiction. It follows that $(a, b) = 1$.

Clearly $c = m^2 + n^2$ is positive. The assumption that $m > n$ shows that $b > 0$. Since m and n are positive, a is positive.
We have thus shown that a, b, c is a fundamental solution. ■

These four lemmas together give us a precise characterization of **Pythagorean triangles**.

Theorem 16.1 *All solutions $x = a$, $y = b$, $z = c$ to $x^2 + y^2 = z^2$, where a, b, c are positive integers and have no common factor, and a is even, are given by*

$$\begin{aligned} a &= 2mn, \\ b &= m^2 - n^2, \\ c &= m^2 + n^2, \end{aligned}$$

where m and n are any relatively prime positive integers, not both odd, and $m > n$.

- *All other integer solutions to $x^2 + y^2 = z^2$ are given by multiples of solutions of the type given in Theorem 16.1.*

Problem Given r, find s such that $r^2 + s^2$ is a square.

Solution

- If r is odd, then $r = m^2 - n^2 = (m - n)(m + n)$ for some integers m, n. Hence write r as the product of two numbers (in any possible way), let the smaller factor be $m - n$ and the larger one $m + n$, and use Theorem 16.1. In this case r plays the role of b.
- If r is even, let $r = 2k$ and find k. If
  - ⋆ k is odd, see the case where r is odd, find a solution and multiply by 2;
  - ⋆ k is even, write k as a product of an even number and an odd number (possibly 1), let the larger be m and the smaller be n. Then $r = 2mn$. Let $s = m^2 - n^2$. In this case r plays the role of a in Theorem 16.1.

    Or: factor out more (or all) even factors and write $r = 2^k \cdot r'$, where $r' > 1$; proceed as before.

Examples

1. Let $r = 13$. Then $r = 13 \cdot 1$, so let $m - n = 1$, $m + n = 13$. Then $m = 7$ and $n = 6$. Let $s = 2mn = 84$. (Check: $84^2 + 13^2 = 7225 = 85^2$ – a fundamental triangle.)

2. Let $r = 14$. Then $r = \mathbf{2} \cdot 7$. Let $r' = 7 = 7 \cdot 1$, so let $m + n = 7$ and $m - n = 1$. Then $m = 4$ and $n = 3$. Let $s' = 2mn = 24$, so $s = \mathbf{2}s' = 48$. (Check: $14^2 + 48^2 = 2500 = 50^2$ – not a fundamental triangle because we multiplied r' and s' by 2 to get r and s.)

3. Let $r = 12$. Then $r = 2 \cdot 2 \cdot 3$ and r plays the role of a in Theorem 16.1. Let $m = 3$ and $n = 2$. Then s plays the role of b, so $s = m^2 - n^2 = 5$. (Check: $12^2 + 5^2 = 169 = 13^2$ – a fundamental triangle.)

   Or: Let $r = \mathbf{4} \cdot 3$, and say $r' = 3$. Then $r' = 3 \cdot 1$, so let $m + n = 3$, $m - n = 1$. Then $m = 2$ and $n = 1$, so $s' = 2mn = 4$ and $s = \mathbf{4}s' = 16$. (Check: $16^2 + 12^2 = 400 = 20^2$.)