Problem 9. Find the only Pythagorean triplet (a, b, c), for which $a + b + c = 1000$.

Or, equivalently, find *all* Pythagorean triplets (a, b, c) with $a + b + c = 1000$. The value 1000 is of course arbitrary, so we discuss the more general problem of finding all Pythagorean triplets with $a + b + c = s$ for some s.
It can easily be seen that for every Pythagorean triplet $a \geqslant 3$ and $a + b + c$ is even, you might want to prove that yourself.

9.1 The straightforward approach

The most straightforward approach is to simply loop over a and b and then check whether $a^2 + b^2 = (s - a - b)^2$. From the condition $a < b < c$, we conclude that $a \leqslant {}^{(s-3)}\!/_{3}$ and $b < {}^{(s-a)}\!/_{2}$.
That approach would lead to code along the lines of

```
s := 1000   // or whatever the perimeter should be
for a := 3 to (s-3) div 3
    for b := (a+1) to (s-1-a) div 2
        c := s-a-b
        if c*c = a*a + b*b then
            output (a,b,c)
        end if
    end for
end for
```

This algorithm is sufficiently fast for small enough s, but it doesn't scale well. If you multiply the value of s by a factor k, the span of each of the two loops is multiplied by the same factor and since the loops are nested, the number of cases to check is multiplied by k^2. So if s is doubled, the programme takes approximately four times as long and increasing the perimeter s by a factor of 10 increases the run time by a factor of approximately 100.

With a little work, you can find better bounds for the loops, thus considerably speeding the algorithm up, but it will still have the same scaling behaviour. This algorithm is definitely unsuitable for perimeters $s \geqslant 1\,000\,000$.

9.2 Using a parametrisation of Pythagorean triplets

A Pythagorean triplet (a, b, c) is by definition *primitive* if $\gcd(a, b, c) = 1$. Since for Pythagorean triplets one has $\gcd(a, b) = \gcd(b, c) = \gcd(c, a)$, such a triplet

is primitive if and only if $\gcd(a, b) = 1$. As was already known to the ancient Greeks, all primitive Pythagorean triplets can be represented as

$$a = m^2 - n^2, \quad b = 2 \cdot m \cdot n, \quad c = m^2 + n^2, \tag{9.1}$$

with $m > n > 0$, perhaps exchanging a and b to have $a < b$. These formulae always produce a Pythagorean triplet, but it will be primitive if and only if exactly one of m, n is even and $\gcd(m, n) = 1$.

From any Pythagorean triplet you get a primitive one by dividing out the greatest common divisor, so every Pythagorean triplet has a *unique* representation

$$a = (m^2 - n^2) \cdot d, \quad b = 2 \cdot m \cdot n \cdot d, \quad c = (m^2 + n^2) \cdot d, \tag{9.2}$$

with $m > n > 0$, $\gcd(m, n) = 1$ and exactly one of m, n even – d is the greatest common divisor of a, b and c.

Using that parametrisation we see

$$a + b + c = 2 \cdot m \cdot (m + n) \cdot d. \tag{9.3}$$

So to find a Pythagorean triplet (a, b, c) with $a + b + c = s$, we have to find a divisor m (> 1) of $s/2$ and an odd divisor k $(= m + n)$ of $s/2m$ with $m < k < 2m$ and $\gcd(m, k) = 1$. Then set $n = k - m$, $d = s/2mk$ and plug these into (9.2).

A fairly simple implementation of that algorithm might look like

```
s2 := s div 2
mlimit := ⌈√s2⌉ − 1
for m := 2 to mlimit
    if s2 mod m = 0 then
        sm := s2 div m
        while sm mod 2 = 0  // reduce the search space by
            sm := sm div 2  // removing all factors 2
        end while
        if m mod 2 = 1 then k := m+2 else k := m+1
        while k < 2*m and k ⩽ sm
            if sm mod k = 0 and gcd(k,m) = 1 then
                d := s2 div (k*m)
                n := k-m
                a := d*(m*m-n*n)
                b := 2*d*m*n
                c := d*(m*m+n*n)
                output (a,b,c)
            end if
            k := k+2
        end while
    end if
end for
```


Author: daniel.is.fischer

where $\lceil\ \rceil$ is the *ceiling* function, i.e. $\lceil x \rceil$ is the smallest integer $i \geqslant x$. This implementation is rather fast and scales well, $s \leqslant 10^{10}$ are processed in fractions of a second. However, at the expense of more complicated code, it can still be improved a bit by making use of the primefactorisation of $s/2$.

9.3 The parametrisation of Pythagorean triplets

9.3.1 Verification of the conditions for primitive triplets

Let us repeat the conditions:
The Pythagorean triplet $(a, b, c) = (m^2 - n^2, 2mn, m^2 + n^2)$, $m > n > 0$ is primitive if and only if $\gcd(m, n) = 1$ and exactly one of m and n is even.

If $\gcd(m, n) = d > 1$, then obviously d^2 is a common divisor of a, b and c, and if m and n are both odd, a, b and c are all even, so the conditions are necessary.

On the other hand, if exactly one of m and n is even and the triplet is *not* primitive, let p be a prime dividing a, b and c. Since a and c are odd, so is p. Any odd prime dividing b must divide at least one of m and n, say p divides m. Then p also divides m^2. But as p also divides $c = m^2 + n^2$, p divides n^2 (and n), too. From that follows $\gcd(m, n) > 1$ and thus the sufficiency of the conditions.

9.3.2 Derivation of the parametrisation

Let $T = (a, b, c)$ be a Pythagorean triplet and $x = a/c$, $y = b/c$. Then (x, y) is a point on the unit circle with rational coordinates and all triplets obtained from T by multiplying a, b and c with the same rational number—and only these—will lead to the same point. Conversely, if $x = p/q$, $y = r/q$ are positive rational numbers with $x^2 + y^2 = 1$, then (p, r, q) is a Pythagorean triplet (not necessarily with $a < b$). Now consider a straight line with positive slope s passing through $(0, -1)$. A parametrisation of that line is given by $(t, s \cdot t - 1)$, $t \in \mathbb{R}$. The second point of intersection of that line and the unit circle is obtained by solving the equation

$$t^2 + (s \cdot t - 1)^2 = 1. \tag{9.4}$$

Rearranging this equation leads to $(s^2 + 1) \cdot t^2 = 2st$. The nonzero solution is thus $t_1 = (2s)/(s^2 + 1)$ and the intersection then has coordinates $x = t_1$ and $y = s \cdot t_1 - 1 = (s^2 - 1)/(s^2 + 1)$. It can be seen that both coordinates are rational and positive if and only if s is rational and greater than 1. So if $s = m/n$ with $m > n > 0$ then $x = (2mn)/(m^2 + n^2)$, $y = (m^2 - n^2)/(m^2 + n^2)$ and we obtain the Pythagorean triplet $(a, b, c) = (2mn, m^2 - n^2, m^2 + n^2)$.

If we start with a primitive triplet (a, b, c), the slope of the line passing through $(0, -1)$ and $\left({}^{a}\!/\!_{c}, {}^{b}\!/\!_{c}\right)$ is ${}^{(b+c)}\!/\!_{a} = {}^{m}\!/\!_{n}$, where the second is the reduced form, i.e. $\gcd(m, n) = 1$. Then $T = (2mn, m^2 - n^2, m^2 + n^2)$ is a multiple of (a, b, c).

If m and n have different parity, we're done, because then T is also primitive as we saw above, therefore it follows that $T = (a, b, c)$.

If m and n are both odd, let $u = {}^{(m+n)}\!/\!_{2}$, $v = {}^{(m-n)}\!/\!_{2}$. Since m and n are odd and $m = u + v$, $n = u - v$, one of u and v is even, the other odd, and $\gcd(u, v) = 1$. Further

$$\begin{aligned} 2mn &= 2(u+v)(u-v) = 2(u^2 - v^2) \\ &\Rightarrow mn = u^2 - v^2, \\ m^2 - n^2 &= (u^2 + 2uv + v^2) - (u^2 - 2uv + v^2) = 4uv \\ &\Rightarrow \frac{m^2 - n^2}{2} = 2uv, \\ m^2 + n^2 &= (u^2 + 2uv + v^2) + (u^2 - 2uv + v^2) = 2(u^2 + v^2) \\ &\Rightarrow \frac{m^2 + n^2}{2} = u^2 + v^2, \end{aligned} \tag{9.5}$$

so $T_1 = (u^2 - v^2, 2uv, u^2 + v^2)$ is a primitive triplet which is also a multiple of (a, b, c), hence $T_1 = (a, b, c)$.