An application of program derivation techniques to 18th-century mathematics

dedicated to Prof. Dr F.E.J. Kruseman Aretz

A. Bijlsma

Department of Mathematics and Computing Science
Eindhoven University of Technology
P.O. Box 513, 5600 MB Eindhoven, The Netherlands
lexb@win.tue.nl

Abstract. Program derivation methodology is applied to reconstruct Euler's proof that every prime congruent to 1 modulo 4 is the sum of two squares.

1 Introduction

This note presents a derivation of one of the proofs given by Euler [4] of the famous theorem that every prime congruent to 1 modulo 4 is the sum of two squares—an observation commonly credited to Fermat but attributed to Girard [5] in [2]. The proof seems to be of methodological interest because it demonstrates that the techniques for program derivation developed by computing science have matured to a level where a proof that originally took many years to find may now be constructed with a minimum of invention. Incidentally, the proof also furnishes a counterexample to Dijkstra's remark [3] that all known methods of factorization are nonconstructive. (It does so because writing a prime as $x^2 + y^2$ is equivalent to factorizing it as $(x + i \cdot y) \cdot (x - i \cdot y)$ in $\mathbf{Z}[i]$.) Of course, this note does not provide any information on the way mathematics was actually done in the 18th century.

In what follows, we shall depart from established mathematical notation in one respect. The assertion that x and y differ by a multiple of k will be written as

$$x =_k y$$

rather than

$$x \equiv y \pmod{k} \quad .$$

There are two reasons for this decision: the classical notation is too confusing in the presence of logical equivalence, and equational reasoning demands an infix operator for the equivalence relation involved. The use of an equality sign is acceptable since a weak form of Leibniz' rule is present: if f is a polynomial over the integers,

$$x =_k y \;\Rightarrow\; f.x =_k f.y \tag{1}$$

for integer x, y and positive integer k.

2 First approximation

We are looking for a constructive proof: given a prime p with $p =_4 1$, we want to find x, y such that

$$x^2 + y^2 = p \quad . \tag{2}$$

(It is not difficult to show [1] that (2) determines x, y uniquely up to minus signs and interchanges, but we shall make no use of this.)

Our first approximation is produced by the most commonly used technique in program derivation: we replace a constant by a variable, and consider

$$P0 : \quad x^2 + y^2 = k \cdot p$$

as invariant of a repetition to be constructed. The chosen constant is acceptable because is easy to see when $P0$ implies the desired postcondition (2), namely when $k = 1$; and because $P0$ is easily initialized, namely by

$$x,\ y,\ k := p,\ 0,\ p \quad .$$

Progress towards the postcondition will be made by decreasing k. In order to be able to take k as the variant function, we strengthen the invariant by

$$P1 : \quad k \geq 1 \quad .$$

3 Invariance of *P*0

To be able to guarantee invariance of $P0$ as k is decreased, we need a method to transform a sum of two squares into a smaller one, while retaining the divisibility by p. Here our starting point is the observation that a sum of two squares constitutes the square of the absolute value of a complex number. This gives

$$\begin{array}{ll}
 & (x^2 + y^2) \cdot (u^2 + v^2) \\
= & \qquad \{\text{introduce complex numbers}\} \\
 & |x + i \cdot y|^2 \cdot |u + i \cdot v|^2 \\
= & \qquad \{\text{distribution}\} \\
 & |(x + i \cdot y) \cdot (u + i \cdot v)|^2 \\
= & \qquad \{\text{multiplication}\} \\
 & |(x \cdot u - y \cdot v) + i \cdot (x \cdot v + y \cdot u)|^2 \\
= & \qquad \{\text{eliminate complex numbers}\} \\
 & (x \cdot u - y \cdot v)^2 + (x \cdot v + y \cdot u)^2 \quad ,
\end{array}$$

so

$$(x^2 + y^2) \cdot (u^2 + v^2) = (x \cdot u - y \cdot v)^2 + (x \cdot v + y \cdot u)^2 \quad . \tag{3}$$

To number theorists, the occurrence of this identity does not come as a surprise: in fact, it constitutes the proof of the theorem that the set of sums of two squares is closed under multiplication, which logically and chronologically precedes Girard's theorem.

Inspired by (3), we investigate an assignment of the form

$$x,\ y := x \cdot u - y \cdot v,\ x \cdot v + y \cdot u \quad .$$

For any k', we have

$$\begin{array}{ll}
 & P0(k,\ x,\ y := k',\ x \cdot u - y \cdot v,\ x \cdot v + y \cdot u) \\
\equiv & \qquad \{\text{substitution}\} \\
 & (x \cdot u - y \cdot v)^2 + (x \cdot v + y \cdot u)^2 = k' \cdot p \\
\equiv & \qquad \{(3)\} \\
 & (x^2 + y^2) \cdot (u^2 + v^2) = k' \cdot p \\
\equiv & \qquad \{P0\} \\
 & k \cdot p \cdot (u^2 + v^2) = k' \cdot p \\
\equiv & \qquad \{\} \\
 & k' = k \cdot (u^2 + v^2) \quad .
\end{array}$$

We conclude that, for arbitrary u, v, predicate $P0$ is invariant under

$$k,\ x,\ y := k \cdot (u^2 + v^2),\ x \cdot u - y \cdot v,\ x \cdot v + y \cdot u \quad .$$

Because this assignment must decrease k, we are led to the condition

$$u^2 + v^2 < 1 \quad . \tag{4}$$

Equation (4) does not have any interesting solutions in integers, since $u, v = 0, 0$ is hopeless in view of $P1$. However, there is no need for u and v to be integer: the derivation given above works equally well for rational u and v, provided the expressions on the right hand side of the assignment are integers. Let us formalize this condition: putting $u = a/c$ and $v = b/c$, we find that the values assigned to x, y, k are integers if

$$c \mid x \cdot a - y \cdot b \quad , \tag{5}$$

$$c \mid x \cdot b + y \cdot a \quad , \tag{6}$$

$$c^2 \mid k \cdot (a^2 + b^2) \quad . \tag{7}$$

(The symbol $\mid$ is pronounced as 'divides'.) In terms of a, b, c, equation (4) may be reformulated as

$$a^2 + b^2 < c^2 \quad . \tag{8}$$

To ensure invariance of $P0$ while decreasing k, it suffices to find a solution to (5) through (8) and then to perform the assignment

$$k,\ x,\ y := k \cdot (a^2 + b^2)/c^2,\ (x \cdot a - y \cdot b)/c,\ (x \cdot b + y \cdot a)/c \quad .$$

First we look at (7). There, c must not be chosen relatively prime to k: if it is, it follows that

$$\begin{array}{ll}
 & (7) \\
\equiv & \qquad \{\}
\end{array}$$

$$\begin{array}{ll}
 & c^2 \mid k \cdot (a^2 + b^2) \\
\equiv & \qquad \{c \text{ and } k \text{ relatively prime}\} \\
 & c^2 \mid a^2 + b^2 \\
\equiv & \qquad \{(8)\} \\
 & a^2 + b^2 = 0 \quad ,
\end{array}$$

and we have already rejected this solution in view of $P1$. Hence c and k must have a nontrivial factor in common. But since we know nothing of the multiplicative structure of k, and indeed k may well be prime, the obvious way to achieve this is to take $c = k$. With this choice, we have

$$\begin{array}{ll}
 & (7) \\
\equiv & \qquad \{c = k\} \\
 & k \mid a^2 + b^2 \\
\equiv & \qquad \{\} \\
 & a^2 + b^2 =_k 0 \\
\equiv & \qquad \{P0, \text{ as the only relevant information on } k \text{ we have}\} \\
 & a^2 + b^2 =_k x^2 + y^2 \\
\Leftarrow & \qquad \{(1)\} \\
 & a =_k y \ \wedge \ b =_k x \quad .
\end{array}$$

In the last line, we might equally well have decided to associate a with x and b with y, as is suggested by the order of the alphabet. However, consideration of (5) shows why we have made the right choice.

$$\begin{array}{ll}
 & (5) \\
\equiv & \qquad \{c = k\} \\
 & k \mid x \cdot a - y \cdot b \\
\equiv & \qquad \{\} \\
 & x \cdot a - y \cdot b =_k 0 \\
\equiv & \qquad \{\} \\
 & x \cdot a - y \cdot b =_k x \cdot y - y \cdot x \\
\Leftarrow & \qquad \{(1)\} \\
 & a =_k y \ \wedge \ b =_k x \quad .
\end{array}$$

And we are in luck, for also

$$\begin{array}{ll}
 & (6) \\
\equiv & \qquad \{c = k\} \\
 & k \mid x \cdot b + y \cdot a \\
\equiv & \qquad \{\} \\
 & x \cdot b + y \cdot a =_k 0 \\
\equiv & \qquad \{P0\} \\
 & x \cdot b + y \cdot a =_k x^2 + y^2 \\
\Leftarrow & \qquad \{(1)\} \\
 & a =_k y \ \wedge \ b =_k x \quad .
\end{array}$$

The choice $c = k$ thus allows us to dispense with (5) through (7), provided we take a and b such that $a =_k y$ and $b =_k x$. We are left with (8).

$$
\begin{array}{ll}
 & (8) \\
\equiv & \qquad \{c = k\} \\
 & a^2 + b^2 < k^2 \\
\Leftarrow & \qquad \{\text{dividing the obligation equally between } a \text{ and } b\} \\
 & |a| < k/\sqrt{2} \ \wedge \ |b| < k/\sqrt{2} \quad .
\end{array}
$$

We conclude that equations (5) through (8) are satisfied if a and b are chosen such that

$$a =_k y \ \wedge \ |a| < k/\sqrt{2} \quad , \tag{9}$$

$$b =_k x \ \wedge \ |b| < k/\sqrt{2} \quad . \tag{10}$$

An explicit solution of (9) and (10) is easy to find: for instance, one of several solutions of (9) is given by

$$a = \begin{cases} y \ \mathbf{mod}\ k & \text{if } y \ \mathbf{mod}\ k < k/2 \quad , \\ y \ \mathbf{mod}\ k - k & \text{if } y \ \mathbf{mod}\ k \geq k/2 \quad . \end{cases}$$

However, we have no need for a definition that is any more specific than (9).

The conclusion of the preceding calculations may be formulated as follows: k is decreased and $P0$ is kept invariant by the statements

$$
\begin{array}{l}
\ \ a : \quad a =_k y \ \wedge \ |a| < k/\sqrt{2} \\
; b : \quad b =_k x \ \wedge \ |b| < k/\sqrt{2} \\
; k,\ x,\ y := (a^2 + b^2)/k,\ (x \cdot a - y \cdot b)/k,\ (x \cdot b + y \cdot a)/k \quad .
\end{array}
$$

4 Invariance of *P*1

For a and b chosen as in the preceding section, we have

$$k \mid a^2 + b^2 \quad , \tag{11}$$

$$a =_k y \ \wedge \ b =_k x \quad . \tag{12}$$

Under assumption of (11), (12), and (the repetition's guard) $k \neq 1$, we have

$$
\begin{array}{ll}
 & P1(k := (a^2 + b^2)/k) \\
\equiv & \qquad \{\text{substitution}\} \\
 & (a^2 + b^2)/k \geq 1 \\
\equiv & \qquad \{(11)\} \\
 & \neg(a^2 + b^2 = 0) \\
\equiv & \qquad \{\} \\
 & \neg(a = 0 \ \wedge \ b = 0) \\
\Leftarrow & \qquad \{(12)\} \\
 & \neg(k \mid x \ \wedge \ k \mid y) \\
\Leftarrow & \qquad \{\} \\
 & \neg(k^2 \mid x^2 + y^2) \\
\equiv & \qquad \{P0\}
\end{array}
$$

$$\begin{array}{ll}
 & \neg(k^2 \mid k \cdot p) \\
\equiv & \qquad \{\} \\
 & \neg(k \mid p) \\
\Leftarrow & \qquad \{k \neq 1 \text{ and } p \text{ is prime}\} \\
 & k \neq p \quad .
\end{array}$$

Since it is very difficult to ensure invariance of $k \neq p$ under $k := (a^2 + b^2)/k$, we decide to strengthen the invariant of the repetition by

$$P2: \quad k < p \quad .$$

As we have already shown k to decrease in each iteration, invariance of $P2$ is trivial. However, the original initialization does not establish $P2$ and we are forced to replace it.

5 Initialization

The standard way to construct an initialization is to choose an 'easy' value, say 0 or 1, for one of the variables, and to calculate the corresponding values of the other variables. In the case under consideration, choosing $k = 1$ is useless, since that takes us back to the original postcondition. The problem being symmetric in x and y, it suffices to consider start values for y.

Initialization of $P0..2$ with $y = 0$ turns out to be impossible, as the diligent reader can easily check. So we consider $y = 1$. This leads to

$$\begin{array}{ll}
 & P0(y := 1) \\
\equiv & \qquad \{\text{substitution}\} \\
 & x^2 + 1 = k \cdot p \\
\equiv & \qquad \{\} \\
 & x^2 =_p -1 \ \wedge \ k = (x^2 + 1)/p \quad .
\end{array}$$

Hence $k := (x^2 + 1)/p$ establishes $P0(y := 1)$ provided x is chosen such that $x^2 =_p -1$. This value of k is obviously positive, so $P1$ is established as well. As to $P2$, we have

$$\begin{array}{ll}
 & (k < p)(k := (x^2 + 1)/p) \\
\equiv & \qquad \{\text{substitution}\} \\
 & x^2 + 1 < p^2 \\
\Leftarrow & \qquad \{(p-1)^2 + 1 < p^2 \text{ since } p \geq 2\} \\
 & 1 \leq x < p \quad .
\end{array}$$

Our final proof obligation is the existence of an x satisfying

$$1 \leq x < p \ \wedge \ x^2 =_p -1 \quad . \tag{13}$$

Here our derivation could end, for it so happens that the existence of an x satisfying (13) is a very famous theorem in number theory, known as the First

Supplement to the Law of Quadratic Reprocity. But for completeness' sake, we supply a proof—one that was originally devised by Lagrange [6].

When we look at the proof obligation (13), the property $(=_p -1)$ brings to mind *Wilson's theorem:* for prime p,

$$(p-1)! =_p -1 \quad . \tag{14}$$

(An easy proof can be found in, for instance, [1].) Taking Wilson's theorem as our point of departure, we have for odd p, with n short for $(p-1)/2$,

$$\begin{array}{ll}
 & -1\\
=_p & \qquad \{(14)\}\\
 & (p-1)!\\
= & \qquad \{\text{definition of factorial}\}\\
 & (\mathit{\Pi}\, j : 1 \leq j < p : j)\\
= & \qquad \{\text{domain split}\}\\
 & (\mathit{\Pi}\, j : 1 \leq j \leq n : j) \cdot (\mathit{\Pi}\, j : n < j < p : j)\\
= & \qquad \{\text{factorial} \parallel \text{dummy transformation } j := p-j\}\\
 & n! \cdot (\mathit{\Pi}\, j : 0 < j < p-n : p-j)\\
= & \qquad \{n = p-n-1\}\\
 & n! \cdot (\mathit{\Pi}\, j : 1 \leq j \leq n : p-j)\\
=_p & \qquad \{p-j =_p -j\}\\
 & n! \cdot (\mathit{\Pi}\, j : 1 \leq j \leq n : -j)\\
= & \qquad \{\text{distribution of } - \text{ over } \mathit{\Pi}\}\\
 & n! \cdot (-1)^n \cdot (\mathit{\Pi}\, j : 1 \leq j \leq n : j)\\
= & \qquad \{\text{factorial}\}\\
 & (-1)^n \cdot n!^2\\
= & \qquad \{\text{provided } p =_4 1\}\\
 & n!^2 \quad .
\end{array}$$

Notice that the last step in the derivation is the first time that the condition $p =_4 1$ plays a role.

We conclude that (13) is established by the assignment

$$x := ((p-1)/2)!\ \mathbf{mod}\ p$$

for p a prime with $p =_4 1$. Inserting this into the algorithm, we obtain the following constructive proof:

```
  $x := ((p-1)/2)!\ \mathbf{mod}\ p$
; $k := (x^2+1)/p$
; $y := 1$
; {inv $P0:\ \ x^2+y^2 = k \cdot p$ ,
       $P1:\ \ k \geq 1$ ,
       $P2:\ \ k < p$ ;
   bd $k$
  }
  $\mathbf{do}\ k \neq 1 \ \rightarrow\ a:\ \ a =_k y \ \wedge\ |a| < k/\sqrt{2}$
```

```
                ; $b :\quad b =_k x \ \wedge\ |b| < k/\sqrt{2}$
                ; $k,\ x,\ y := (a^2 + b^2)/k,\ (x \cdot a - y \cdot b)/k,\ (x \cdot b + y \cdot a)/k$
        od .
```

Acknowledgement The ETAC read a previous version of this note and suggested several improvements in the presentation.

References

1. H. Davenport, *The higher arithmetic*, 6th ed. Cambridge University Press, 1992.
2. L.E. Dickson, *History of the theory of numbers*, vol. II. Carnegie Institute, Washington, 1919. Repr. Chelsea, New York, 1966.
3. E.W. Dijkstra, *A derivation of a proof by D. Zagier*. EWD1154, August 1993.
4. L. Euler, 'Novae demonstrationes circa resolutionem numerorum in quadrata'. *Acta Eruditorium Lipsiae* (1773), 193.
5. A. Girard (ed.), *L'Arithmétique de Simon Stevin*. Leiden, 1625.
6. J.L. Lagrange, 'Démonstration d'un théorème nouveau concernant les nombres premiers', *Nouv. Mém. Acad. Roy. Berlin* **2** (1773), 125–337.