FACTORING WITH CUBIC INTEGERS

J. M. POLLARD

SUMMARY. We describe an experimental factoring method for numbers of form $x^3 + k$; at present we have used only $k = 2$. The method is the cubic version of the idea given by Coppersmith, Odlyzko and Schroeppel (Algorithmica 1 (1986), 1–15), in their section 'Gaussian integers'. We look for pairs of small coprime integers a and b such that:

i. the integer $a + bx$ is smooth,

ii. the algebraic integer $a + bz$ is smooth, where $z^3 = -k$. This is the same as asking that its norm, the integer $a^3 - kb^3$ shall be smooth (at least, it is when $k = 2$).

We used the method to repeat the factorisation of F_7 on an 8-bit computer ($2F_7 = x^3 + 2$, where $x = 2^{43}$).

INTRODUCTION

We consider the case $k = 2$ throughout. We denote by $\mathbf{Z}$ the set of rational integers (ordinary integers) and by S the set of algebraic integers:

$$[a, b, c] = a + bz + cz^2, \qquad (a, b, c \text{ in } \mathbf{Z}).$$

These constitute the algebraic integers of the field generated by z, and possess the property of unique factorisation (neither statement true for general k, see e. g. [2]). According to [1], such methods are still possible when unique factorisation fails.

We also write:

$$\{a, b, c\} = a + bx + cx^2.$$

When ii. holds, we have some factorisation:

$$[a, b, 0] = [d, e, f] \cdot \ldots,$$

into units and primes of S (defined shortly). Then also:

$$\{a, b, 0\} \equiv \{d, e, f\} \cdot \ldots \pmod n.$$

But by i. we have also a factorisation:

$$\{a, b, 0\} = p \cdot q \cdot \ldots,$$

into small primes of $\mathbf{Z}$. So we have a congruence (mod n) involving rational integers from two small sets. From a sufficient number of such congruences, we obtain some equations:

$$X^2 \equiv Y^2 \pmod n,$$

and hopefully the factorisation of n.

1991 *Mathematics Subject Classification.* Primary 11Y05, 11Y40.

Key words and phrases. Factoring algorithm, algebraic number fields.

PROPERTIES OF THE SET S

The norm of a member $[a, b, c]$ of S is the rational integer:

$$N(a, b, c) = a^3 - 2b^3 + 4c^3 + 6abc.$$

This is a multiplicative function, i. e. the equation

$$[a, b, c] = [d, e, f] \cdot [g, h, i] \tag{1}$$

implies:

$$N(a, b, c) = N(d, e, f) \cdot N(g, h, i).$$

Given an equation (1), we say that $[d, e, f]$ divides $[a, b, c]$.

The norm can be zero only when $a = b = c = 0$. Numbers with norm $+1$ or -1 are called *units*. There are an infinity of units, namely all the numbers:

$$\pm U^i \quad (i = 0, \pm 1, \pm 2, \dots),$$

where $U = [1, 1, 0]$. We give a table of the small powers of U:

i	U^i	U^{-i}
0	$[1, 0, 0]$	$[1, 0, 0]$
1	$[1, 1, 0]$	$[-1, 1, -1]$
2	$[1, 2, 1]$	$[5, -4, 3]$
3	$[-1, 3, 3]$	$[-19, 15, -12]$
4	$[-7, 2, 6]$	$[73, -58, 46]$

A unit divides any integer. If $[d, e, f]$ in (1) is a unit, then the other two numbers are termed *associates*; clearly this means that:

$$N(a, b, c) = \pm N(g, h, i),$$

but the converse statement is false as we shall see.

A number $[a, b, c]$ is termed *prime* if any factorisation (1) contains a unit (and an associate). A number of norm $\pm p$ (p prime) is certainly a prime; but not all primes are of this form.

A rational prime p need not be a prime of S. We have $N(p, 0, 0) = p^3$, so perhaps p can have prime factors of norm $\pm p$ or $\pm p^2$. Indeed it can. There are four cases (see [2, p. 186]):

1. The primes $p = 2$ and 3. These factor as a unit and the cube of a prime of norm p:

$$\begin{aligned} 2 &= -1 \cdot [0, 1, 0]^3, \\ 3 &= [1, 1, 0] \cdot [-1, 1, 0]^3. \end{aligned}$$

2. Primes p of form $6m + 1$, with -2 a cubic residue (mod p):

$$p = 31,\ 43,\ 109,\ 127,\ 157,\ \dots.$$