Notes on J. Pollard's paper,
"Factoring with Cubic Integers."

Eric Bach
February 14, 2003

Pollard works with the real cubic field $K = \mathbf{Q}(\alpha)$, with $\alpha = \sqrt[3]{-2}$. In working with any algebraic number field there are some standard questions to ask, so we do this first.

What is the ring of integers?

The minimal polynomial for α is $f(X) = X^2 + 2$, and we compute

$$\text{disc}(f) = \text{resultant}(f, f') = 108 = 2^2 \cdot 3^3.$$

Since α is an algebraic integer, we know that Δ, the discriminant of K, has to be one of

$$\pm 108, \pm 27, \pm 12, \pm 3.$$

The Minkowski discriminant bound for $n = 3$ tells us that

$$|\Delta| \geq \frac{n^{2n}}{(n!)^2} = \frac{3^6}{(6!)^2} = 20.25,$$

so 12 and 3 (with either sign) are out. To eliminate 27 we can consider $p = 2$. We notice that $(-\alpha)^3 = 2$, so if P is a prime above 2, it must divide 2 to the third power. This tells us that 2 is ramified. By Dedekind's theorem (a prime ramifies iff it divides the field discriminant), 2 divides Δ. So we have

$$\Delta = \pm 108.$$

Therefore the ring of integers is $\mathbf{Z}[\alpha]$. We will call this O_K.

What is the exact discriminant?

We know everything except the sign of Δ. Here is one way to get it. The algebraic integers $1, \alpha, \alpha^2$ are linearly independent over $\mathbf{Q}$, so we have $\text{disc}(1, \alpha, \alpha^2) = f^2\Delta$, for some integer f. We then compute

$$\text{disc}(1, \alpha, \alpha^2) = \det \begin{pmatrix} 1 & \alpha & \alpha^2 \\ 1 & \zeta\alpha & \zeta^2\alpha^2 \\ 1 & \zeta^2\alpha & \zeta\alpha^2 \end{pmatrix}^2 = -108.$$

So $\Delta = -108 < 0$. (Note that it is relatively easy to determine the sign.)

What's the class number?

Minkowski proved that every ideal class has a representative A with $NA \leq c|\Delta|^{1/2}$, where

$$c = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s,$$

for a field of degree n with $2s$ complex embeddings into $\mathbf{C}$. The bound works out to $NA \leq 2.9404....$ There is only one ideal lying above 2 (we showed that 2 is totally ramified), and it is principal. So the class number is 1.

How do primes split?

Let p be a prime in $\mathbf{Z}$. The ideal $(p) = pO_K$ has a factorization

$$(p) = P_1^{e_1} \cdots P_r^{e_r}.$$

Furthermore, O_K/P_i is a finite field of order p^{f_i}. The game is to figure out r, and the e_i's and f_i's. We know priori that $3 = \sum e_i f_i$.

The ramified primes are 2 and 3. We have already determined that $(2) = P_2^3$ (totally ramified). The prime 3 has to be a product of a degree 1 and degree 2 prime, or the third power of a degree 1 prime. The degrees follow the factorization of $X^3 + 2$ in the 3-adic field, and we notice that $X^3 + 2$ has no zero in $\mathbf{Z}/9$. So 3 is also totally ramified.

For a prime that does not divide Δ, the degrees are the same as those of the irreducible factors of $X^3 + 2$ mod p. From this we find that:

1. If $p \equiv 1$ mod 6 and -2 is a cube mod p, then $X^3 + 2$ has 3 linear factors mod p. So p splits completely: $(p) = P_1P_2P_3$.
2. If $p \equiv 1$ mod 6 and -2 is not a cube mod p, then $X^3 + 2$ is irreducible mod p. So p is inert: $(p) = P$.
3. If $p \not\equiv 1$ mod 6, then $X^3 + 2$ has exactly one root mod p. So p is the product of a degree 1 and a degree 2 prime ideal: $(p) = P_1P_2$.

What is the norm?

The norm of an element β is the determinant of the multiplication-by-β map. Working this out, we get

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

We can check this by another computation, using facts about our specific field. If

$$\beta = a + b\alpha + c\alpha^2$$

then its conjugates are

$$\beta' = a + b\zeta\alpha + c\zeta^2\alpha^2$$

and

$$\beta'' = a + b\zeta^2\alpha + c\zeta\alpha^2$$

Here ζ is a primitive cube root of unity. Multiplying these together and simplifying, we get the formula above.

A useful lemma.

Lemma: the coefficients of any algebraic integer β in the "box"

$$|\beta| \leq A, |\beta'| \leq B$$

are bounded in absolute value by $(A + 2B)/3$. Note that this implies that the number of integers in the box is finite.

To prove this we use a gadget called the *dual basis*. Let

$$\gamma_1 = 1, \gamma_2 = \alpha, \gamma_3 = \alpha^2.$$

Further define

$$\gamma_1^* = 1/3, \gamma_2^* = -\alpha^2/6, \gamma_3^* = \alpha/6.$$

These have the nice property that

$$\text{Trace}(\gamma_i \gamma_j^*) = \delta_{ij}.$$

Now, suppose that $\beta = \sum a_i \gamma_i$ is as above. Then we compute

$$|a_i| = |\text{Trace}(\beta \gamma_i^*)| = |\beta \gamma_i^* + \beta'(\gamma_i^*)' + \beta''(\gamma_i^*)''|$$

$$\leq \max(\ \gamma_i^*\text{'s conjugates })(A + 2B) \leq (A + 2B)/3.$$

What are the units?

Consider the *logarithmic embedding*

$$L : \epsilon \mapsto (\log|\epsilon|, 2\log|\epsilon'|).$$

which takes O^* into $\mathbf{R}^2$. All roots of unity map to 0. Are there any other units in the kernel? For such a unit η, all of its conjugates would have to have absolute value 1, and by the lemma, its powers cannot all be distinct. So there must be some multiplicative relation of the form $\eta^r = \eta^s$. This gives $\eta^{r-s} = 1$, so η is a root of unity.

That is the image? Using the lemma, we see that it must be a discrete subgroup of $\mathbf{R}^2$, hence isomorphic to $\mathbf{Z}^r$ for $r \leq 2$. The number r is called the *unit rank*. It cannot be 2 because we have an additive relation, coming from $|N(\epsilon)| = 1$. We look at integral elements with small coefficients, and observe that

$$\epsilon = 1 + \alpha = -0.25992104989$$

is a unit. So $r = 1$.

We now have an exact sequence of Abelian groups

$$0 \to W \to O_K^* \to \mathbf{Z} \to 0.$$

Such sequences must split ($\mathbf{Z}$ is free), so

$$O_K^* \cong W \times \mathbf{Z}.$$

We now prove that every unit is (up to sign) a power of ϵ. Suppose not. Then for some other unit η, we have $\epsilon = \pm\eta^d$ with $d > 1$. The logarithmic embedding of η is

$$(\log|\eta|, 2\log|\eta'|) = (\log|\epsilon|/d, (2/d)\log|\epsilon'|).$$

Since $d \geq 2$, η has to satisfy

$$\log|\eta| \leq \log|\epsilon|/2, \qquad \log|\eta'| \leq \log|\epsilon'|/2.$$

This implies

$$|\eta| \leq \exp(\log|\epsilon|/2) = 1.961459176, \qquad |\eta'| \leq \exp(\log|\epsilon'|/2) = 1.400521037.$$

By the lemma, if $\eta = a + b\alpha + c\alpha^2$, we have the bounds

$$|a|, |b|, |c| \leq (1.961459176 + 2 \times 1.400521037)/3 = 1.587500417.$$

Thus, the coefficients of a fundamental unit must be ≤ 1 in absolute value, and enumerating these, we find nothing that cannot be generated by ϵ.

The "size" of the fundamental unit is measured by the *regulator*. The regulator of our field is

$$R = |\log|\epsilon|| = 1.34737734835.$$

Divisibility testing.

Using the norm, we have a good way to determine if one integer of K divides another. Let $\beta, \gamma \in K$. Then

$$\frac{\beta}{\gamma} = \frac{\beta\gamma'\gamma''}{N(\gamma)},$$

and this is an algebraic integer iff $N(\gamma)$ divides each coefficient of the numerator. Two numbers are associates iff each divides the other.

There is a Euclidean algorithm for O_K. See H. J. Godwin, Quart. J. Math. Oxford (2), v. 18, 1967, pp. 333-338. It is not clear that the use of this is any more efficient than the test above.

Elements of bounded norm.

The goal now is to show that every algebraic integer β of K with small norm has an associate with small coefficients. Consider the maps

$$\begin{array}{ccccc} K^* & \to & \mathbf{R}^2 & \to & \mathbf{R} \\ & L & & S & \end{array}$$

where the first is the log embedding (given by the same formula) and the second just sums coordinates. Thus,

$$SL(\beta) = \log N(\beta).$$

By adjusting the sign if necessary, we can assume this is positive. We will use a particular basis of $\mathbf{R}^2$, namely

$$w = (\log|\epsilon|, 2\log|\epsilon'|),$$
$$v = (1, 2).$$

Then $L(\beta) = \xi v + \eta w$ for real numbers ξ, η. Choose an integer k so that $|\eta - k| \leq 1/2$. Put $\hat{\beta} = \beta\epsilon^{-k}$. Then

$$L(\hat{\beta}) = \xi v + (\eta - k)w = (\xi + (\eta - k)\log|\epsilon|, 2\xi + 2(\eta - k)\log|\epsilon'|).$$

Applying S to the last expression, we see that $\xi = \log N(\beta)/3$. Thus, we have the estimate

$$\log|\hat{\beta}| \leq \frac{\log N(\beta)}{3} + \left|\frac{1}{2}\log|\epsilon|\right|,$$

which implies

$$|\hat{\beta}| \leq 2\sqrt[3]{N(\beta)}.$$

Similarly,

$$2\log|\hat{\beta}'| \leq \frac{2\log N(\beta)}{3} + \log|\epsilon'|,$$

so

$$|\hat{\beta}'| \leq \frac{3}{2}\sqrt[3]{N(\beta)}.$$

Plugging these estimates into the "useful lemma" we see that the coefficients of $\hat{\beta}$ are bounded by

$$\frac{5}{3}\sqrt[3]{N(\beta)}.$$

This gives a nice result: to be guaranteed of finding an associate for each integer of norm $\leq B$, we can look at $\Theta(B)$ algebraic numbers. This bound cannot be improved. To see this, we appeal to the following result. Let $j(B)$ denote the number of ideals of O_K with norm $\leq B$. Then [Lang, Algebraic Number Theory, p. 132]

$$j(B) \sim \kappa B$$

where κ is a constant for the field. (I think it is the residue of K's zeta function at 1.) For our K we have

$$\kappa = \frac{2\pi R}{|\Delta|^{1/2}} = 0.814624.$$

Making the factor bases.

Pollard works with two factor bases:

$$FB_1: \text{ all ordinary primes } p \le B$$

and

$$FB_2: \text{ generators for all degree 1 prime ideals with } NP \le B$$

For convenience, generators for the unit group $(-1, \epsilon)$ are included in FB_2.

Suppose we want m primes in FB_1. By the prime number theorem, $p_m \sim m \log m$, so we should take B to be about this value. The cost to enumerate all the primes $\le B$, by the sieve of Eratosthenes, is

$$\sum_{p \le \sqrt{B}} \frac{B}{p} \sim B \log\log B.$$

Here we have used the prime number theorem. The idea is that the density of primes near n is about 1 in $\log n$, so

$$\sum_{p \le \sqrt{B}} \frac{B}{p} \approx B \sum_{m \le \sqrt{B}} \frac{1}{m \log m} \approx B \int_2^{\sqrt{B}} \frac{dt}{t \log t} \sim B \log\log B.$$

To make FB_2, we appeal to the bound of the last section. Make a list of all numbers $a + b\alpha + c\alpha^2$, with $|a|, |b|, |c| \le \text{const} B^{1/3}$, together with their norms. Sort these by norm, and save those of prime norm. For each prime that appears, find a set of non-associates.

On average, we should expect each ideal to be represented by $\Theta(1)$ associates. (This is of course not guaranteed to happen for primes, since they are a bit sparser.)

Factoring.

To factor $n = x^3 + 2$, Pollard uses the following idea. Look for pairs (a, b) that make $ax + b$ divisible by the primes in FB_1, and also $a\alpha + b$ divisible by the primes in FB_2. Factoring both of these, and taking the sign of $ax + b$ to be positive, we get a "relation"

$$p_1^{e_1} p_2^{e_2} \cdots p_r^{e_4} = ax + b \equiv a\alpha + b = \pi_1^{f_1} \pi_2^{f_2} \cdots \pi_s^{f_s} (-1)^g \epsilon^h.$$

There is a homomorphism ϕ from O_K to $\mathbf{Z}/n$ sending α to x, and the congruence is with respect to its kernel. (Here r and s are the prime counts for the two factor bases.)

If we collect about $r + s + O(1)$ of these relations, we expect that there will be a linear dependence among the exponents, when taken mod 2. Combining the relations in the usual way, we obtain

$$c^2 \equiv \delta^2 \equiv d^2,$$

where $c = \phi(\delta)$. If we are lucky then $\gcd(c \pm d, n)$ is a nontrivial factor of n.

Sieving linear forms.

We can rapidly find smooth values of $ax + b$ as follows. Suppose we are willing to try all $|a| \le C$, $1 \le b \le D$. For each b, we do the following.

for $a = -C \ldots C$: $L_a = \log|ax + b|$.
for all prime powers $q \le B$ (here $q = p^e$)
    $a_0 = -bx \bmod q$
    for $i = (-C - a_0)/q \ldots (C - a_0)/q$
        $a = a_0 + iq$
        $L_a = L_a - \log p$
output all a with $L_a \approx 0$, and try to factor $ax + b$ over FB_1.

By considerations similar to the prime number sieve, we will use $\Theta(CD \log\log B)$ time to do this.

What is the "harvest"? The probability of smoothness is approximated by the Dickman rho function. This is a special function, defined by the integral equation.

$$\rho(\lambda) = \begin{cases} 1, & \text{if } 0 \le \lambda \le 1; \\ \frac{1}{\lambda}\int_{\lambda-1}^{\lambda} \rho(t)dt, & \text{if } \lambda > 1. \end{cases}$$

The probability that a random integer near m is B-smooth is about $\rho(\lambda)$, with

$$\lambda = \frac{\log m}{\log B}.$$

If C and D are small compared to $x = n^{1/3}$ we would expect to get about

$$\rho\left(\frac{\log n}{3\log B}\right) \times 2CD \times \zeta(2)^{-1}$$

pairs in this manner. Pollard actually only used pairs for which a and b are relatively prime, and the probability that this holds is $1/\zeta(2) = 61\%$.

To speed up his program, Pollard also included a "large prime" enhancement. The analog of the ρ function for this situation can be computed as indicated in the following paper: E. Bach and R. Peralta, Asymptotic Semi-smoothness Probabilities, Math. Comp. 1996.

Nothing special is used to factor the $a\alpha + b$ values. The norm of each is computed, and factored over FB_1. If the norm is smooth, then for each p in FB_1, divide by the (at most 3) primes of that norm in FB_2. Assuming that smoothness of $N(a\alpha + b)$ is independent of the smoothness of $ax + b$ (a big if!), we expect

$$\rho\left(\frac{3\log(C + D)}{\log B}\right),$$

of them to be smooth. (Actually one should average over values of a and b, and think carefully about the norm; I am just using $(C + D)^3$ as a crude estimate for $N(a\alpha + b)$.)

This suggests a total yield of about

$$\frac{2}{\zeta(2)}\ \rho\left(\frac{\log(C + D)}{\log B}\right)\rho\left(\frac{\log n}{3\log B}\right)CD$$

relations.

This is in the right ballpark: Pollard used $C = 2000$, $D = 4800$, and $B = 3571$ to factor $n = 2^{129} + 2$. Our yield formula evaluates to 3795, and there actually were 1671 relations.