

$t_2 \equiv -t_1 \pmod{p^\beta}$ (t_1 and t_2 are not necessarily in the range from $[\sqrt{n}] + 1$ to $[\sqrt{n}] + A$).

5. Still with the same value of p , run down the list of $t^2 - n$ from part 2. In a column under p put a 1 next to all values of $t^2 - n$ for which t differs from t_1 by a multiple of p , change the 1 to a 2 next to all values of $t^2 - n$ for which t differs from t_1 by a multiple of p^2 , change the 2 to a 3 next to all values of $t^2 - n$ for which t differs from t_1 by a multiple of p^3 , and so on until p^β . Then do the same with t_1 replaced by t_2 . The largest integer that appears in this column will be β .

6. As you go through the procedure in 5), each time you put down a 1 or change a 1 to a 2, a 2 to a 3, etc., divide the corresponding $t^2 - n$ by p and keep a record of what's left.

7. In the column $p = 2$, if $n \not\equiv 1 \pmod{8}$, then simply put a 1 next to the $t^2 - n$ for t odd and divide the corresponding $t^2 - n$ by 2. If $n \equiv 1 \pmod{8}$, then solve the equation $t^2 \equiv n \pmod{2^\beta}$ and proceed exactly as in the case of odd p (except that there will be 4 different solutions t_1, t_2, t_3, t_4 modulo 2^β if $\beta \geq 3$).

8. When you finish with all primes $\leq P$, throw out all of the $t^2 - n$ except for those which have become 1 after division by all the powers of $p \leq P$. You will have a table of the form in Example 9 in §3, in which the column labeled b_i will have the values of $t, [\sqrt{n}] + 1 \leq t \leq [\sqrt{n}] + A$, for which $t^2 - n$ is a B -number, and the other columns will correspond to all values of $p \leq P$ for which n is a quadratic residue.

9. The rest of the procedure is exactly as in §3.

Example. Let us try to factor $n = 1042387$, taking the bounds $P = 50$ and $A = 500$. Here $[\sqrt{n}] = 1020$. Our factor base consists of the 8 primes $\{2, 3, 11, 17, 19, 23, 43, 47\}$ for which 1042387 is a quadratic residue. Since $n \not\equiv 1 \pmod{8}$, the column corresponding to $p = 2$ alternates between 1 and 0, with a 1 beside all odd t , $1021 \leq t \leq 1520$.

We describe in detail how to form the column under $p = 3$. We want a solution $t_1 = t_{1,0} + t_{1,1} \cdot 3 + t_{1,2} \cdot 3^2 + \cdots + t_{1,\beta-1} \cdot 3^{\beta-1}$ to $t_1^2 \equiv 1042387 \pmod{3^\beta}$, where $t_{1,j} \in \{0, 1, 2\}$ (for the other solution t_2 we can take $t_2 = 3^\beta - t_1$). We can obviously take $t_{1,0} = 1$. (For each of our 8 primes the first step — solving $t_1^2 \equiv 1042387 \pmod{p}$ — can be done quickly by trial and error; if we were working with larger primes, we could use the procedure described at the end of §II.2.) Next, we work modulo 9: $(1 + 3t_{1,1})^2 \equiv 1042387 \equiv 7 \pmod{9}$, i.e., $6t_{1,1} \equiv 6 \pmod{9}$, i.e., $2t_{1,1} \equiv 2 \pmod{3}$, so $t_{1,1} = 1$. Next, modulo 27: $(1 + 3 + 9t_{1,2})^2 \equiv 1042387 \equiv 25 \pmod{27}$, i.e., $16 + 18t_{1,2} \equiv 25 \pmod{27}$, i.e., $2t_{1,2} \equiv 1 \pmod{3}$, so $t_{1,2} = 2$. Then modulo 81: $(1 + 3 + 18 + 27t_{1,3})^2 \equiv 1042387 \equiv 79 \pmod{81}$, which leads to $t_{1,3} = 0$. Continuing until 3^7 , we find the solution (in the notation of §I.1 for numbers written to the base 3): $t_1 \equiv (210211)_3 \pmod{3^7}$, and $t_2 \equiv (2012012)_3 \pmod{3^7}$. However, there is no t between 1021 and 1520 which is $\equiv t_1$ or t_2 modulo 3^7 . Thus, we have $\beta = 6$, and we can take $t_1 = (210211)_3 = 589 \equiv 1318 \pmod{3^6}$ and $t_2 = 3^6 - t_1 = 140 \equiv$