

More Errata for Factorization and Primality Testing

Dale Brownawell

page 4, lines 18-20 Just because the exponent is at least 2 doesn’t imply that it is even. To complete this argument easily, I need Theorem 1.4:

By the identity of line 13, any prime $p$ dividing $(z - x)/2$ divides $m$. Therefore $p$ occurs to an even power in $m^2$, by Theorem 1.4, and not at all in $(z + x)/2$. Consequently by Theorem 1.4 again, $p$ occurs to the same (even) power in $m^2$ and in $(z - x)/2$. In this way we see that $(z - x)/2$ is a perfect square and that $(z + x)/2$ is a perfect square.

page 10, line 5 The case $a = b = 0$ needs to be dealt with separately by defining $\gcd(0, 0) := 0$. (2 Sept 97)

page 12, line 12 Superfluous period page 12, lines 14, 15 This doesn’t work when $x$ is zero, i.e. when $a = b$ above. So begin this with the test $\textbf{IF } x \neq 0$ (29 Sep 97)

page 18, line 9 from bottom The actual number is 50 847 534. Bressoud’s number comes from a table computed by Meissel in the last century (quite a feat for the time!), which has been reproduced in many places. Meissel modified Legendre’s formula

\[ 1 + \pi(x) = \pi(\sqrt{x}) + |x| - \sum_{p_i \leq \sqrt{x}} \left\lfloor \frac{x}{p_i} \right\rfloor + \sum_{p_i < p_j < \sqrt{x}} \left\lfloor \frac{x}{p_i p_j} \right\rfloor - \sum_{p_i < p_j < p_k \leq \sqrt{x}} \left\lfloor \frac{x}{p_i p_j p_k} \right\rfloor + \ldots \]

to make it more convenient for calculation. In 1958, D.H. Lehmer introduced a further refinement of this formula and recalculated the range to find the correct number given here. (7 September 1997)

page 20, line 5 Superfluous period

page 24, line 16 Missing comma

page 27, line 7 Superfluous period

page 28, lines 2, 3 Since $\lfloor \sqrt{x} \rfloor$ is the exact function, I would rather ask this in two parts:

- What is the exact formula for the number of integers $\leq x$ which are perfect squares?
- What is a continuous function of $x$ which is asymptotic to this formula?

(16 September 1997)

page 28, Problem 2.10 has several interpretations. The one Bressoud expects is probably: “How many of these 100 numbers are prime? How does this compare with the expected number?”

1
A much harder interpretation is: “How many primes (distinct primes) appear in the factorizations of your choice of these 100 numbers. How does this compare ...” (6 September 2001)

page 29, Problem 2.15 The meaning of the phrase “trial division up to 5000” is ambiguous. Under Algorithm 2.4, all the numbers up to 25,000,000 can be factored using trial division with primes up to 5,000.
There are two possible versions of the this problem, depending on the interpretation given the pharase, and each runs counter to something said or done previously in the book.
Interpretation 1: How large a number can “usually” be factored into a product of primes, each of size less than 5,000? Here the computation from Problem 2.9 involving seven digit numbers may provide evidence. However this intepretation of the phrase runs counter to the usage in line 21, page 21.
Interpretation 2: How large a number can “usually” be factored into a product of primes by using trial division by primes up to 5,000? Here the interval must start above 25,000,000, and the computation from Problem 2.9 is irrelevant, contrary to the statement on lines 20-21, page 28. (15 Sep 1997)

page 34, lines 6,8 These lines mean that one should reduce the product MOD m to end up with a number in the set \{0, 1, \ldots, m-1\}. (16 Sep 1997)

page 38, line 11 Theorem 3.7 is intended, not 3.1.

page 40, Problem 3.8 This is a hard problem because two basic things have not been made explicit yet:

- \(\phi(q)\) is even unless \(q = 1, 2\).
- Every common divisor of \(m, n\) divides \(gcd(m, n)\).

page 40, l. -1 Note that this chokes when \(n = 0\) because then \(b_0\) is never not created. So start with \(b_0 \leftarrow 0\). (18 Sep 2001)

page 41 FOR \(i = 0\) to \(k\) DO (16 Sep 1997)

page 49, lines 13,14,18 Thinspace missing after \(mod\).

page 49, lines 14,18 I do not like this notation, since it seems to mix moduli. In other words, I would repeat the \(a\)'s in the first column of these displayed lines as well.

page 51, lines 11,12,13 Equality should be replaced by \(\leftarrow\).

page 65, line 17 \(x_{i+1} = f(x_i) = x_i^2 + c\)

p.66, line -7 Replace 5 by \(4 + c\).
Strictly speaking, this is not correct. Namely when \( p \) is an odd prime and \( n = p^e \) with \( e = 2, 3 \). The problem is that it is difficult to make the heuristic argument concerning the distribution of the factors of between \( x - y \) and \( x + y \) precise for the cases when \( \gcd(n, (x^2 - y^2)/n) \neq 1 \). I calculated the exact probabilities, but it took several pages. Of course, powers are easy to detect, so maybe you want to exclude them. Maybe you even want to exclude pairs \( \{(x, y) : \gcd(xy, n) \neq 1\} \).

Since this is used in Theorem 6.5, it might be better to spell this out now with the following remark.

**Lemma 1.** The gcd of any two factors from the right of equation (2.6) is a power of 2.

**Proof.** Let \( p \) be an odd prime. Clearly if \( p | (m^t - 1) \), then the remaining factors are congruence to 2 modulo \( p \). Similarly, if

\[
b^{2^iT} \equiv -1 \pmod{p} \implies \begin{cases} b^{2^iT} \not\equiv \pm 1 \pmod{p}, & \text{rm for } e < i \\ b^{2^iT} \equiv 1 \pmod{p}, & \text{rm for } e > i \end{cases}
\]

\[\square\]

\(19\) Oct 97

There needs to be some space before “is”.

Twice if \( p \neq 2 \).

I don’t recall that this has been shown. Claim If \( p \) is odd and \( p^e | (m^{n-1} - 1), e > 0 \), then \( p^e \) divides a unique factor

\[m^n - 1, m^n + 1, m^{2n} + 1, \ldots, m^{2^{e-1}n} + 1.\]

Namely it divides the \( j \)th factor if \( j \) is minimal such that

\[p | (m^{2^j n} - 1) = (m^t - 1)(m^t + 1) \ldots (m^{2^{j-1}t} + 1),\]

since by the remark from page 76, \( p \) divides no other factor. 19 Oct 97

Test for the base (The other terminology was never introduced.)
It might be worth mentioning here that, by a similar argument,
\[ m^{2^\min\{b,k\}} \equiv 1 \pmod{q}. \]
Thus by the minimality of \( k \), \( k \leq b \) and \( b = k \). (16 Oct 97)

The case \( a = 3 \) and \( a' = 1 \) was omitted inadvertently. (29 Oct 2002)

This requires the restriction that BOTH integers be odd, so replace \( n \) here by \( m' \).

Replace \( n \) by \( m' \)

I find this line misleading. By definition, each \( g(r) \) is congruent to \( r^2 \), so the displayed line follows directly from the last displayed line on the preceding page. As is said in the sentence before, what is new is that a subproduct of the \( g(r_i) \) is exactly a square. It would make more sense to me to write instead something like
\[ r_1^{2\delta_1} \times r_2^{2\delta_2} \times \cdots \times r_t^{2\delta_t} \equiv p_1^{2b_1} \times p_2^{2b_2} \times \cdots \times p_s^{2b_s}, \]
where each \( \delta = 0 \) or \( 1 \), and \( s = 1229 \), and both sides of the congruence are perfect squares.

"close" to \( 2k\sqrt{n} \)

I would make this sentence more specific: But it will still take almost a million \( r \)'s to obtain 1230 completely factored integers involving only the first 1229 primes and thereby allow us to find non-trivial solution of \( x^2 \equiv y^2 \) modulo a 25-digit integer.

I would be more specific here as well: ... is to not check for high divisibility by primes and to compensate by not requiring that the prime factors \( p \) which we obtain for \( f(r) \) have logarithms whose sum be terribly close to that of \( f(r) \) before testing \( f(r) \) for factorization over the selected factor base.

Since we will not be getting to Lucas sequences in our one-semester course, I give here a short derivation of Tonelli’s Method based instead on primitive roots. This is an adaptation of the discussion of the approach in the book *Algorithmic Number Theory* by E. Bach and J. Shalit, MIT, 1996, page 156. We use the fact that we shall establish later in the course:

**Theorem 1.** If \( p \) is a prime, then \( p \) admits a primitive root.

Now finding a primitive root \( g \) for \( p \) is hard. We will use properties of \( g \) to establish the correctness of the procedure; the ultimate algorithm will not depend
on $g$. There is no problem taking square roots modulo 2, so let $p$ be an odd prime, say $p - 1 = 2^t t$, $t$ odd. Fix $b$, a quadratic non-residue modulo $p$, $1 < b < p - 1$.

**Lemma 2.** Then for every number $a$, $1 \leq n < p$, there is a unique pair of integers $(i, j)$, $0 \leq i < 2^s$, $0 \leq j < t$, such that $a \equiv b^i \cdot g^{j2^s}$ mod $p$.

**Proof:** To see this, notice that the products on the right give $2^t t = p - 1$ integers not divisible by $p$. If two of them were congruent modulo $p$, then cancelling the smaller powers of $b$ and $g^{2^s}$ from both sides would give a congruence of the form

$$b^i \equiv g^{j2^s} \mod p.$$  

As the exponents are unique modulo the order of $g$, i.e. modulo $p - 1$, we see that $il \equiv j \cdot 2^s$ mod $2^t t$. But $l$ is odd and $i < 2^s$, so $il \not\equiv j \cdot 2^s$ mod $2^s$. We have arrived at an impossibility, and this establishes the Lemma.  

We think about computing the square root of $b^i$ and $g^{j2^s}$ mod $p$ separately. The second one is (in a sense) easy, but we have to be sure not to cheat and use the representation in terms of $g$. Here is the trick:

$$(g^{j2^s})^{t+1} \equiv (g^{j2^s})^t \cdot g^{j2^s} \equiv (g^{2^s})^j \cdot g^{j2^s} \equiv g^{j2^s} \mod p,$$

and $t + 1$ is even! So one square root is given by:

$$\sqrt{g^{j2^s}} \equiv (g^{j2^s})^{(p+1)/2} \mod p.$$  

Unfortunately, this representation is still not yet solely in terms of $a$.

Putting this worry aside for the moment, we try to find the square root of $b^i$ mod $p$, $0 \leq i < 2^s$ used in the expression of $a$ itself. We know that $\alpha$ such that $a = g^\alpha$ is even ($a$ is a quadratic residue modulo $p$), while $\beta$ such that for $b = g^\beta$ is odd ($b$ is a quadratic non-residue modulo $p$). We determine $i$ recursively modulo higher and higher powers of 2 via $i_k := i \mod 2^k$, $k = 1, 2, \ldots, s$, where $i_k$ satisfies

$$\alpha - \beta \cdot i_k \equiv 0 \mod 2^k, \quad i_1 = 2.$$  

If $\alpha + \beta \cdot i_{k-1} \equiv 0 \mod 2^k$, then let $i_k := i_{k-1}$. Otherwise $\alpha - \beta \cdot i_{k-1} \equiv 2^{k-1} \mod 2^k$, so let $i_k = i_{k-1} - 2^{k-1}$. As $\beta$ is odd, this is the unique choice modulo $2^k$ guaranteeing that

$$a/b^{i_k} \equiv g^{i_k \cdot 2^k} \mod p, \quad \text{for some } l_k, \ 0 \leq l_k < 2^{s-k} \cdot t$$  

or, more to the point,

$$(a/b^{i_k})^{2^{s-k} t} \equiv 1 \mod p.$$  

It is this recurrence which finally frees us from $g'$! We solve it using at most $s$ tests along the way as $k = 2, 3, \ldots, s$. Knowing $i := i_s$ solves all our problems:

- The square root of $b^i$ is obtained as $\sqrt{b^i} := b^{i/2} \mod p$.
- $g^{j2^s}$ is determined by $g^{j2^s} \equiv a/b^i \mod p$.
- A square root of $a$ is obtained as $\sqrt{a} = b^{i/2} \cdot (a/b^i)^{(s+1)/2} \mod p$.

Remarks: Now Tonelli’s Method can be thought of in two ways. If we just search with $b = 2, 3, \ldots$, it is deterministic, but with no knowledge of how long the search will take for an unspecified $p$. If we choose $b$ randomly, then the likelihood is 50% that the first choice will work. So a random search finds a quadratic nonresidue
quickly with high probability. Having chosen $b$, Tonelli’s algorithm finishes off the
job in $O((\log p)^3)$ bit operations.

page 110, line 10 J. Gerver As far as I recall, references always furnished a first
name or at least an initial. I think it would look better if this were consistent.

page 111, lines 17,18 ..a vector of zeros indexed by the $r$ to which we add $\log p$ in
the $r$th place when ... If we are sieving over $2M$ values of $r$, then ...

page 111, line 19 This statement is not really true. Consider for example the values
generated when $i$ is very close to $M$. It would be better to say that “the logarithm
of ... will be bounded by, say”

$$\text{TARGET} = (\log n)/2 + \log M + \log 3.$$ 
or “on average will be approximately”.

page 111, line -4 is to attempt trial factorization of $f(r)$ over our factor base if
the $r$th entry of our vector is close enough to the \text{TARGET}, where “close enough” is
specified as

page 111, line -1 I think it would be helpful to insert here, that, as long as $\log M <
T \times \log(p_{max})$, as it is in practice, then we will always be attempting Trial Division
on all $f(r)$ for which the product of all distinct prime divisors from the factor base
is at least $\sqrt{n}$.

page 111, line 18 According to Carl Pomerance’s, The number field sieve, in Proc.
Symp. Appl. Math. 48 (1994), AMS, 465-480, $M$ should of the same order of
magnitude as $exp(\sqrt{(\log n)(\log \log n)})$.

page 112, line 1 I think it would be worthwhile to point out that the density of
square-free numbers is $6/\pi^2$, so that we could expect to pick up a fixed fraction
of the $g(r)$ which factor completely over our factor basis even without following
Silverman’s suggestion.

Sam Wagstaff says that he sieves by $27, 3^4, 5^3, 7^2, \ldots, 23^2, 29^1, \ldots$. If my arith-
metic is right, this accounts for over 96 per cent of all sufficiently large integers.

page 112, line -5 I don’t see this. It seems to me to be

$$t - (\text{SQRT} - M) \mod p \text{ or } p + t - (\text{SQRT}) - M \mod p,$$
depending on whether $t > (\text{SQRT} - M) \mod p$ or not. Similarly the “other”
solution of (8.2) then leads us to add $\log p$ in the $p - t - (\text{SQRT} - M) \mod p$ or
$2p - t - (\text{SQRT} - M) \mod p$ place, depending on whether $t + (\text{SQRT} - M) \mod p \leq p$
or not, and every $p$ place thereafter.

page 116,line 12 Question: What are the statistics or heuristics on the odds, or is
it just the density of square-free integers?
page 116, line 22 ...strings, ignoring now the (even) contributions from the large prime at the end, will add up ...

page 116, line 26 vectors

page 116, line 27 Davis, Holdridge, and Simmons report that, under ideal conditions, consideration of extra factors can speed up the process of finding enough complete factorizations by a factor of six.

page 117, line 6 The function $a \times F(r)$ producing the numbers to be factored ...

page 117 How can one choose the arithmetic progressions to minimize overlaps?

page 118 Replace “Holdright” by “Holdridge”.

Problem 8.6. We need to know a quantitative form of Dirichlet’s Theorem to conclude that we get about half the primes when $n$ is not a perfect square.

page 119, Problem 8.5 Amend so that $M$ is small with respect to $n$, and replace “usually” by “on average”.

page 121, The situation of 8.12 is a bit confusing. I have the following suggestions:

- line 1 ... and the solutions of the congruence
- line 3 are exactly those $x \equiv \pm t \mod 2^{n-1}$, then the solutions of the congruence
- line 5 are either those $x \equiv \pm t \mod 2^n$ or else those $x \equiv 2^{n-1} \pm t \mod 2^n$.

page 125, line 15 We need a result on page 129 (lines 2/3) that best belongs here, I feel. Then the former Corollary 9.3 becomes a corollary of this one.

Corollary 9.3 If $b$ has order $e$ modulo $n$, then

$$b, b^2, \ldots, b^e$$

are distinct modulo $n$.

Proof. Since $\gcd(b, n) = 1$, there is a multiplicative inverse $c$ such that $b \times c \equiv 1 \mod n$. If $b^i \equiv b^j \mod n$, $0 < i \leq j \leq e$, then

$$1 \equiv b^i \times c^i \mod n \equiv b^{(j-i)}b^i c^i \mod n \equiv b^{(j-i)} \mod n.$$  

Since $0 \leq j - i < e$, we see by Theorem 9.1 that $j = i$. Q.E.D.

---

page 126, lines 14 - 19. Let $e'$ denote the order of $b^i \mod n$. Then by definition of order and by Theorem 9.1, $ie'$ is the least multiple of $i$ which is also a multiple of $e$, i.e. $ie' = \text{lcm}(e, i)$.

page 129, line 3 I don’t see this directly, unless $d = p - 1$. To deduce it from the current Corollary 9.3 seems harder than deducing it directly from Theorem 9.1. See page 125.
If $l < 2^k$, then $2 \cdot 2^l | F(k) - 1$. Thus $2^l \cdot m = \frac{F(k)-1}{2}$ and
$$5 \frac{F(k)-1}{2} \equiv (5^2)^m \equiv \mod F(k).$$

$p > F = \frac{n}{R} - \frac{1}{R} > \sqrt{n} - \frac{1}{R}$
and
$$p + 1 \geq F + 1 > \sqrt{n} + (1 - \frac{1}{R}) > \sqrt{n}.$$

The book does not establish the relevant property of binomial coefficients: Set
$$\phi := (p-1)p^{k-2}$$
and denote $\text{ord}_p n := \max\{e : p^e \mid n\}$. Since
$$\binom{\phi}{i} = \frac{\phi \cdot (\phi - 1) \ldots (\phi - i + 1)}{i \cdot 1 \ldots (i - 1)},$$
we see that $\text{ord}_p j = \text{ord}_p \phi - j$ for $j < \phi$. Thus $\text{ord}_p \binom{\phi}{i} = k - 2 - \text{ord}_p i$. So Bressoud’s claim translates to $k + i - 2 - \text{ord}_p i \geq k$, or $i - 2 \geq \text{ord}_p i$, when $i \geq 2$. Recall that $p$ is odd, so $p \geq 3$, and the claim will hold if $3^{i-2} \geq i$, which is true for $i \geq 3$.

Bressoud means
$$4a^3 + 27b^2 \neq 0$$
line 16
and
$$0 = x^3 + ax + b.$$In general, for fixed $a, b$, there will be two choices of $z$ for which (13.3) does not have distinct roots.

It is easy to see that 417 is divisible by 3. Instead the entry should be 419.