

A low complexity probabilistic test for integer multiplication

Dima Grigoriev

CNRS, Mathématiques, Université de Lille
59655, Villeneuve d'Ascq, France
dmitry.grigoryev@math.univ-lille1.fr
<http://logic.pdmi.ras.ru/~grigorev>

Gérald Tenenbaum

Institut Élie Cartan,
Université Henri Poincaré-Nancy
BP 239 54506 Vandœuvre, France
gerald.tenenbaum@iecn.u-nancy.fr
<http://www.iecn.u-nancy.fr/~tenenb>

(version 4/12/2009, 0h57)

Abstract

A probabilistic test for equality $a = bc$ for given n -bit integers a, b, c is designed within complexity $n(\log \log n) \exp\{O(\log^* n)\}$.

Keywords. probabilistic test, integer multiplication, small divisors

1 Test for multiplication

Denote by $M(n)$ the complexity of multiplication of two n -bit integers. It is well-known [4] that

$$M(n) = n(\log n) \exp\{O(\log^* n)\},$$

improving upon the algorithm given in [6].¹

We consider here probabilistic testing of the equality $a = bc$ for given n -bit integers a, b, c . In this context, it may be worth mentioning that a probabilistic test for matrix product $A = BC$ within linear complexity has been described in [3]. A general concept of a checking problem (vs. a solving one) was suggested in [2].

Lemma 1.1. *The complexity of division with remainder of n -bit integer a by m -bit integer d does not exceed $n(\log m) \exp\{O(\log^* m)\}$.*

Proof. Let $a \in \mathbb{N}^*$ be an n -bit integer and, for $1 \leq m \leq n$, write the 2^m -ary expansion of a , namely $a = \sum_{0 \leq i \leq n/m} a_i 2^{mi}$ with $0 \leq a_i < 2^m$ ($1 \leq i \leq n/m$). Each of remainder $u_i := \text{Rem}(2^{mi}, d) \in [0, d[$ may be computed within complexity $O(M(m))$ [1]. Subsequently one can calculate each $v_i := \text{Rem}(a_i u_i, d)$ ($1 \leq i \leq n/m$) again within complexity $O(M(m))$. Finally, $\text{Rem}(\sum_{0 \leq i \leq n/m} v_i, d)$ can be computed within complexity $O(n)$. \square

To perform a probabilistic test of the validity of the equation $a = bc$, the algorithm picks randomly an integer $2 \leq d \leq n^2$, calculates $a' := \text{Rem}(a, d)$,

¹Recall the definition $\log^* n := \min\{j \geq 0 : \log^{[j]} n \leq 1\}$, where $\log^{[j]}$ is the j -fold iteration of the logarithm to the base 2, denoted by \log .

$b' := \text{Rem}(b, d)$, $c' := \text{Rem}(c, d)$ and finally tests the equality $a' = \text{Rem}(b'c', d)$. This test has complexity less than $n(\log \log n) \exp\{O(\log^* n)\}$ by virtue of Lemma 1.1 and has an error less than $1/2$ due to the following result applied to $a - bc$.

Theorem 1.2. *Let $\delta > 1 - \ln 2$. Then any sufficiently large n -bit integer has at most δn^2 divisors in the interval $[1, n^2]$.*

Remark 1.3. *More precisely, the bounds established in the next section show that, for any $\varepsilon > 0$, the test can be defined by picking the random divisor d in the interval $[2, n^{\sqrt{e}+\varepsilon}]$, but not by picking d in the interval $[2, n^{\sqrt{e}-\varepsilon}]$.*

2 Bounds for the number of small divisors

We designate by \ln_k the k -fold iteration of the Neperian logarithm function $\ln = \ln_1$.

Let $P(n)$ denote the largest prime factor of an integer $n > 1$, with the convention that $P(1) = 1$. For $x \geq 1$, $y \geq 1$, we define $S(x, y) := \{n \leq x : P(n) \leq y\}$ as the set of y -friable integers not exceeding x , and denote by $\Psi(x, y)$ its cardinality. We designate by ϱ Dickman's function, which is defined as the unique continuous solution on \mathbb{R}^+ of the difference-differential equation

$$u\varrho'(u) + \varrho(u-1) = 0 \quad (u > 1)$$

with initial condition $\varrho(u) = 1$ ($0 \leq u \leq 1$). The function ϱ is strictly decreasing from 1 to 0 on $[0, \infty[$ and we have

$$\varrho(u) = u^{-u+o(u)} \quad (u \rightarrow \infty).$$

For further information and references on the Dickman function, see, e.g., [7], chapter III.5.

Given a function $Z : [1, \infty[\rightarrow]1, \infty[$ such that $\ln Z(x) = o(\ln x \ln_2 x)$ as $x \rightarrow \infty$ and a real number $t > e$, we let $\Xi(t; Z)$ denote the smallest solution in $]1, \infty[$ of the equation

$$Z(x)\varrho\left(\frac{\ln x}{\ln_2 t}\right) = 1.$$

That such a solution exists follows from the fact that the right hand side is > 1 for $x = \ln t$ and tends to 0 as $x \rightarrow \infty$.

Put

$$\tau(n, x) := \sum_{\substack{d|n \\ d \leq x}} 1 \quad (n \in \mathbb{N}^*, x \geq 1).$$

Theorem 2.1. *Let $Z : [1, \infty[\rightarrow]1, \infty[$ be a non-decreasing function satisfying*

$$(1) \quad \ln Z(x) \ll (\ln x)/(\ln_2 3x)^2 \quad (x \geq 1).$$

For all $\varepsilon > 0$ and sufficiently large n , we have

$$(2) \quad x > \Xi(n; (1 + \varepsilon)Z) \Rightarrow \tau(n, x) \leq x/Z(x).$$

Under the extra condition

$$(3) \quad \ln Z(x) = o(\sqrt{\ln x}) \quad (x \rightarrow \infty),$$

there exists a strictly increasing integer sequence $\{n_k\}_{k=0}^{\infty}$ such that

$$(4) \quad \tau(n_k, x_k) > x_k/Z(x_k) \quad (k \geq 0),$$

with $x_k := \Xi(n_k; (1 - \varepsilon)Z)$.

Before embarking on the proof, we note a simple corollary obtained by considering the case when Z is a constant. For fixed $v > 1$, we let $x_n(v)$ denote the smallest real number such that

$$\tau(n, x) \leq x/v \quad (n \geq 1, x \geq x_n(v)).$$

Theorem 1.2 follows by specializing $v = 2$ in the next statement, and Remark 1.3 by selecting $v = 1/(1 - \ln 2)$.

Theorem 2.2. For $1 < v \leq 1/(1 - \ln 2)$, $w := \exp\{1 - 1/v\}$, we have

$$(5) \quad x_n(v) \leq (\ln n)^{w+o(1)} \quad (n \rightarrow \infty).$$

Moreover, in the above upper bound, the exponent w is optimal in the following sense: given any $\varepsilon > 0$, there exists a strictly increasing integer sequence $\{n_j\}_{j=0}^{\infty}$ such that

$$(6) \quad x_{n_j}(v) > (\ln n_j)^{w-\varepsilon} \quad (j \geq 0).$$

Proof. We select $Z(x) = v$ in Theorem 2.1 and note that, since $\varrho(u) = 1 - \ln u$ for $1 \leq u \leq 2$, we have $\Xi(n; v) = (\log n)^w$ for $n \geq 3$ and $1 < v \leq 1/(1 - \log 2)$. \square

Proof of Theorem 2.1. We first establish (2).

Let p_k denote the k -th prime number and $\{p_j(n)\}_{j=1}^{\omega(n)}$ designate the increasing sequence of distinct prime factors of a natural integer n . Then the mapping

$$F : \prod_{1 \leq j \leq \omega(n)} p_j(n)^{\nu_j} \mapsto \prod_{1 \leq j \leq \omega(n)} p_j^{\nu_j}$$

is an injection from the set of divisors of n into the subset of $p_{\omega(n)}$ -friable integers d . Moreover, $F(d) \leq d$ for all $d \geq 1$. Therefore

$$(7) \quad \tau(n, x) \leq \Psi(x, p_{\omega(n)}) \quad (n \geq 1, x \geq 1).$$

Since we have, for any integer $n \geq 1$,

$$\prod_{p \leq p_{\omega(n)}} p \leq n,$$

a strong form of the prime number theorem yields

$$(8) \quad p_{\omega(n)} \leq L_n := \left\{ 1 + e^{-(\ln_2 n)^c} \right\} \ln n$$

for any $c < 3/5$ and sufficiently large n .

If, for instance, $\ln n \leq e^{2(\ln_2 x)^{11/6}}$, we have, as $n \rightarrow \infty$, by virtue of the uniform upper bound for $\Psi(x, y)$ given in theorem III.5.1 of [7],

$$\Psi(x, L_n) \leq \Psi(x, 2 \ln n) \ll x^{1-1/(2+2 \ln_2 n)} \ll x e^{-\frac{1}{5}(\ln x)/(\ln_2 x)^{11/6}} = o(x/Z(x)).$$

This implies $\tau(n, x) < x/Z(x)$ in this case.

If

$$(9) \quad \ln n > e^{2(\ln_2 x)^{11/6}},$$

Hildebrand's asymptotic formula (see for instance corollary III.5.19 of [7]) implies

$$\Psi(x, L_n) \leq \{1 + o(1)\} x \varrho\left(\frac{\ln x}{\ln L_n}\right) \quad (x \rightarrow \infty).$$

However, by (8), we have

$$\frac{\ln x}{\ln L_n} = \frac{\ln x}{\ln_2 n} + O(e^{-(\ln_2 x)^{11c/6}}).$$

By selecting $\frac{6}{11} < c < \frac{3}{5}$, and in view of the estimate $\varrho'(u) \ll (\ln 2u)\varrho(u)$ ($u \geq 1$) established for instance in corollary III.5.14 of [7], we deduce that

$$\varrho\left(\frac{\ln x}{\ln L_n}\right) \sim \varrho\left(\frac{\ln x}{\ln_2 n}\right)$$

as n and x tend to infinity under condition (9). It follows that, in the same circumstances, we have $\tau(n, x) < x/Z(x)$ as soon as $x > \Xi(n, (1 + \varepsilon)Z)$.

This completes the proof of the upper bound (2).

To prove the lower bound (4), we give ourselves a (large) constant $D \in \mathbb{N}^*$ and put

$$\Psi_D(x, y) := \sum_{\substack{n \leq x \\ p|n \Rightarrow p \leq y}} g_D(n),$$

where g_D is the indicator of D -free integers, i.e. integers such that $p^\nu || n \Rightarrow \nu \leq D$. The arithmetical function g_D is an s -function in the sense of [5], in other words $g_D(n)$ only depends upon

$$s(n) := \prod_{p^\nu || n, \nu \geq 2} p^\nu.$$

Theorem 1 of [5] may hence be applied, and, writing $\zeta(s)$ for the Riemann zeta function, yields, for any $\varepsilon > 0$,

$$(10) \quad \Psi_D(x, y) := \sum_{\substack{n \leq x \\ p|n \Rightarrow p \leq y}} g_D(n) \sim \frac{x \varrho(u)}{\zeta(D+1)}$$

as x and y tend to infinity in such a way that $\exp\{(\log_2 x)^{5/3+\varepsilon}\} \leq y \leq x$.

Let us then put $N_k := \prod_{1 \leq j \leq k} p_j^D$ ($k \geq 1$). Applying (10) for

$$(11) \quad p_k < x \leq \exp\{o((\ln p_k)^2 / \ln_2 p_k)\} \quad (k \rightarrow \infty),$$

and setting $u_k := (\ln x)/\ln p_k$, we get

$$\tau(N_k, x) = \Psi_D(x, p_k) \sim \frac{x \varrho(u_k)}{\zeta(D+1)}.$$

Now, observe that hypothesis (11) implies

$$u_k \ln(1 + u_k) = o(\ln p_k) \quad (k \rightarrow \infty).$$

Since $\ln N_k \sim D p_k$, we therefore have, when x satisfies (11),

$$\begin{aligned} \varrho\left(\frac{\ln x}{\ln_2 N_k}\right) &= \varrho\left(\frac{\ln x}{\ln p_k + O(1)}\right) = \varrho\left(u_k + O\left(\frac{u_k}{\ln p_k}\right)\right) \\ &= \left\{1 + O\left(\frac{u_k \ln(1 + u_k)}{\ln p_k}\right)\right\} \varrho(u_k) \sim \varrho(u_k). \end{aligned}$$

Select $x := \Xi(N_k; (1 - \varepsilon)Z)$, where $\varepsilon \in]0, 1 - 1/Z(1)[$. From the above, it then follows that $Z(x)(1 - \varepsilon)\varrho(u_k) = 1 + o(1)$ as $k \rightarrow \infty$. We deduce, on the one hand, that $x > p_k$, because $\varrho(1) = 1$, and, on the other hand, in view of the classical asymptotic estimates for $\varrho(u)$ (see for instance theorem III.5.13 of [7]), that

$$u_k \ln(1 + u_k) \asymp \ln Z(x) = o(\sqrt{\ln x}).$$

Condition (11) is hence fulfilled. It follows that

$$\tau(N_k, x) = \Psi_D(x, p_k) > \frac{x}{(1 - \varepsilon/2)\zeta(D+1)Z(x)} > \frac{x}{Z(x)} \quad (k \rightarrow \infty),$$

provided we choose, as we may, D sufficiently large in terms of ε .

This completes the proof of the second part of our theorem. \square

As a further concrete example of application of Theorem 2.1, we state the following corollary.

Corollary 2.3. *Let $c > 0$, $\varepsilon > 0$. For sufficiently large n and all*

$$x > (\ln n)^{\{1+\varepsilon\}c(\ln_3 n)/\ln_4 n},$$

we have $\tau(n, x) \leq x/(\ln x)^c$. This statement is optimal in the sense that one cannot replace ε by $-\varepsilon$.

Acknowledgements. The first author is grateful to John Harrison who asked for a deterministic test for multiplication, Pieter Moree for valuable discussions and to Max-Planck Institut für Mathematik, Bonn, where the note has been written, for hospitality.

References

- [1] A. Aho, J. Hopcroft and J. Ullman, *Design and analysis of computer algorithms*, Addison-Wesley, (1974).
- [2] M. Blum, S. Kannan, *Designing programs that check their work*, Proc. ACM Symp. Th. Comput. (1989), 86–97.
- [3] R. Freivalds, *Fast probabilistic algorithms*, Proc. Symp. Math. Found. Comput. Sci., Springer (1979), 57–69.
- [4] M. Fürer, *Faster integer multiplication*, Proc. ACM Symp. Th. Comput., (2007), 57–66.
- [5] A. Ivić and G. Tenenbaum, *Local densities over integers free of large prime factors*, Quart. J. Math. (Oxford) (2) **37** (1986), 401–417.
- [6] A. Schönhage and V. Strassen, *Schnelle Multiplikation grosser Zahlen*, Computing, **7** (1971), 281–292.
- [7] G. Tenenbaum, *Introduction à la théorie analytique et probabiliste des nombres*, third edition, coll. Échelles, Belin (Paris), 2008.