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 11/1/2010, 17h39)

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 $1 \leqslant m \leqslant n$, write the 2^m-ary expansion of a, namely $a = \sum_{0\leqslant i\leqslant n/m} a_i 2^{mi}$ with $0 \leqslant a_i < 2^m$ $(0 \leqslant i \leqslant n/m)$. Each of remainder $u_i := \mathrm{Rem}(2^{mi}, d) \in [0, d[$ may be computed within complexity $O(M(m))$ [1]. Subsequently one can calculate each $v_i := \mathrm{Rem}(a_i u_i, d)$ $(0 \leqslant i \leqslant n/m)$ again within complexity $O(M(m))$. Finally, $\mathrm{Rem}\left(\sum_{0\leqslant i\leqslant n/m} v_i, d\right)$ can be computed within complexity $O(n)$. □

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

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

$b' := \mathrm{Rem}(b,d)$, $c' := \mathrm{Rem}(c,d)$ and finally tests the equality $a' = \mathrm{Rem}(b'c', d)$. 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 $[2, n^{\sqrt{\mathrm{e}}+\varepsilon}]$, but not by picking d in the interval $[2, n^{\sqrt{\mathrm{e}}-\varepsilon}]$.*

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 $x \geqslant 1$, $y \geqslant 1$, we define $S(x,y) := \{n \leqslant x : P(n) \leqslant y\}$ 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

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

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

$$\varrho(u) = u^{-u+o(u)} \qquad (u \to \infty).$$

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

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

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

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 $x \to \infty$.

Put

$$\tau(n,x) := \sum_{\substack{d \mid n \\ d \leqslant x}} 1 \qquad (n \in \mathbb{N}^*,\ x \geqslant 1).$$

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

$$\ln Z(x) \ll (\ln x)/(\ln_2 3x)^2 \qquad (x \geqslant 1). \tag{1}$$

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

$$x > \Xi(n; (1+\varepsilon)Z) \Rightarrow \tau(n,x) \leqslant x/Z(x). \tag{2}$$

Under the extra condition

$$\ln Z(x) = o\big(\sqrt{\ln x}\,\big) \qquad (x \to \infty), \tag{3}$$

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

$$\tau(n_k, x_k) > x_k/Z(x_k) \qquad (k \geqslant 0), \tag{4}$$

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

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

$$\tau(n,x) \leqslant x/v \qquad (n \geqslant 1,\, x \geqslant x_n(v)).$$

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* $1 < v \leqslant 1/(1-\ln 2)$, $w := \exp\{1-1/v\}$*, we have*

$$x_n(v) \leqslant (\ln n)^{w+o(1)} \qquad (n \to \infty). \tag{5}$$

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*

$$x_{n_j}(v) > (\ln n_j)^{w-\varepsilon} \qquad (j \geqslant 0). \tag{6}$$

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

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 an natural integer n. Then the mapping

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

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

$$\tau(n,x) \leqslant \Psi(x, p_{\omega(n)}) \qquad (n \geqslant 1,\, x \geqslant 1). \tag{7}$$

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

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

a strong form of the prime number theorem yields

$$p_{\omega(n)} \leqslant L_n := \Big\{1 + \mathrm{e}^{-(\ln_2 n)^c}\Big\}\ln n \tag{8}$$

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

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

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

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

If

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

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

$$\Psi(x, L_n) \leqslant \{1 + o(1)\} x \varrho\Big(\frac{\ln x}{\ln L_n}\Big) \qquad (x \to \infty).$$

However, by (8), we have

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

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

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

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

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

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

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

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

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

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

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

$$p_k < x \leqslant \exp\{o\big((\ln p_k)^2/\ln_2 p_k\big)\} \qquad (k \to \infty), \tag{11}$$

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

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

Now, observe that hypothesis (11) implies

$$u_k \ln(1+u_k) = o(\ln p_k) \qquad (k \to \infty).$$

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

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

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 $k \to \infty$. 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

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

Condition (11) is hence fulfilled. It follows that

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

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

This completes the proof of the second part of our theorem. □

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 $\tau(n, x) \leqslant x/(\ln x)^c$. 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.