Joachim von zur Gathen & Igor E. Shparlinski (2006). GCD of Random Linear Combinations. *Algorithmica* **46**(1), 137–148. ISSN 0178-4617 (Print), 1432-0541 (Online). URL http://dx.doi.org/10.1007/s00453-006-0072-1.

GCD of Random Linear Combinations

Joachim von zur Gathen
B-IT Computer Security
Universität Bonn
53113 Bonn, Germany
gathen@bit.uni-bonn.de
http://www-math.upb.de/~aggathen

Igor E. Shparlinski
Department of Computing
Macquarie University,
NSW 2109, Australia
igor@comp.mq.edu.au
http://www.comp.mq.edu.au/~igor

April 10, 2005

Abstract

We show that for arbitrary positive integers $a_1, \ldots, a_m$, with probability $6/\pi^2 + o(1)$, the gcd of two linear combinations of these integers with rather small random integer coefficients coincides with $\gcd(a_1, \ldots, a_m)$. This naturally leads to a probabilistic algorithm for computing the gcd of several integers, with probability $6/\pi^2 + o(1)$, via just one gcd of two numbers with about the same size as the initial data (namely the above linear combinations). This algorithm can be repeated to achieve any desired confidence level.

1 Introduction

We let $\mathbf{a} = (a_1, \ldots, a_m) \in \mathbb{N}^m$ be a vector of $m \geq 2$ positive integers, $\mathbf{x} = (x_1, \ldots, x_m), \mathbf{y} = (y_1, \ldots, y_m) \in \mathbb{N}^m$ be two integer vectors of the same length, where $\mathbb{N} = \{1, 2, \ldots\}$, and consider the linear combinations

$$\mathbf{a} \cdot \mathbf{x} = \sum_{1 \leq i \leq m} a_i x_i \qquad \text{and} \qquad \mathbf{a} \cdot \mathbf{y} = \sum_{1 \leq i \leq m} a_i y_i.$$

Then clearly $\gcd(a_1, \ldots, a_m)$ divides $\gcd(\mathbf{a} \cdot \mathbf{x}, \mathbf{a} \cdot \mathbf{y})$, and we want to show that in fact, equality holds quite often.

For a vector $\mathbf{u} = (u_1, \ldots, u_m) \in \mathbb{R}^m$ we define its *height* as

$$h(\mathbf{u}) = \max_{1 \leq i \leq m} |u_i|.$$

For an integer M, we denote by $\rho_{\mathbf{a}}(M)$ the probability that, for $\mathbf{x}, \mathbf{y}$ chosen uniformly in $\mathbb{N}^m$ with height at most M,

$$\gcd(a_1, \ldots, a_m) = \gcd(\mathbf{a} \cdot \mathbf{x}, \mathbf{a} \cdot \mathbf{y}). \tag{1}$$

Assuming that the linear combinations $\mathbf{a} \cdot \mathbf{x}$ and $\mathbf{a} \cdot \mathbf{y}$ behave as random integer multiples of $\gcd(a_1, \ldots, a_m)$, it is reasonable to expect that (1) holds with probability $\zeta(2)^{-1} = 6/\pi^2$ where $\zeta(s)$ is the Riemann zeta function, and indeed we show that this holds asymptotically. In particular, our result implies that one can choose M of order $\ln N$ in the algorithm of [2] rather than of order N as in Corollary 3 of [2], thus reducing quite dramatically the size of the operands which arise in the algorithm of [2].

The lower bound on $\rho_{\mathbf{a}}(M)$ plays a crucial role in the analysis of a fast probabilistic algorithm for computing the gcd of several integers which has been studied [2]. This algorithm, for any $\delta > 0$, requires only about

$$\frac{1}{\ln(\pi^2/(\pi^2 - 6))} \ln \delta^{-1} \approx 1.06802 \cdot \ln \delta^{-1} \tag{2}$$

pairwise gcd computations, to achieve success probability at least $1 - \delta$ (where $\ln z$ is the natural logarithm of $z > 0$). For comparison, it is noted that the naive deterministic approach may require up to $m - 1$ gcd computations. A drawback of that algorithm is that for its proof of correctness, the arguments given to the gcd computations are substantially larger than the original inputs. In [4] we give an asymptotic lower bound on $\rho_{\mathbf{a}}(M)$ (of the expected

order $\zeta(2)^{-1}$) which holds starting with very small values of M. Here we present a completely explicit and slightly stronger form of that result. More importantly, we obtain an asymptotic formula for $\rho_{\mathbf{a}}(M)$ which holds in a wide range of parameters.

Our results now imply that one may choose the operands of the algorithm of [2] of approximately the same size as the inputs. An exact cost analysis depends on the cost of the particular gcd algorithm, a variety of which can be found in [3].

Furthermore, we demonstrate that our result is rather tight and it fails if M is chosen substantially smaller than required for our result.

A well-known fact says that $\gcd(a_1, \dots, a_m) = 1$ with probability $\zeta^{-1}(m)$ for random integers $a_1, \dots, a_m$; see [5], Theorem 332, for a precise formulation in the case $m = 2$. It is important to not confuse our result which holds for arbitrary (that is, "worst-case") inputs with the "average-case" result which follows from this fact.

2 Main Results

We show that $\rho_{\mathbf{a}}(M)$ equals $\zeta(2)^{-1}$ asymptotically in a wide range of parameters. More precisely, we have the following.

Theorem 1. *Let $m \geq 3, \mathbf{a} \in \mathbb{Z}^m$ be of height at most N, and*

$$M \geq \max\{9m, \ln N\}.$$

Then

$$|\rho_{\mathbf{a}}(M) - \zeta(2)^{-1}| \leq \frac{19}{\ln(M/m)}.$$

Proof. As in [2], it is enough to consider only the case where $\gcd(a_1, \dots, a_m) = 1$. We set $Q = \frac{1}{4}\ln(M/m)$, and let $\mathcal{L}$ be the set of all pairs of integer vectors $\mathbf{x}, \mathbf{y} \in \mathbb{N}^m$ with $h(\mathbf{x}), h(\mathbf{y}) \leq M$, where $\mathbb{N} = \{1, 2, \dots\}$ For an integer $k \geq 2$, we denote by $P(k)$ the largest prime divisor of k, and set $P(1) = 1$. We define the following subsets:

- $\mathcal{Q} = \{(\mathbf{x}, \mathbf{y}) \in \mathcal{L} : \ Q \geq P(\gcd(\mathbf{a} \cdot \mathbf{x}, \mathbf{a} \cdot \mathbf{y})) > 1\}$,
- $\mathcal{R} = \{(\mathbf{x}, \mathbf{y}) \in \mathcal{L} : \ M > P(\gcd(\mathbf{a} \cdot \mathbf{x}, \mathbf{a} \cdot \mathbf{y})) > Q\}$,
- $\mathcal{S} = \{(\mathbf{x}, \mathbf{y}) \in \mathcal{L} : \ P(\gcd(\mathbf{a} \cdot \mathbf{x}, \mathbf{a} \cdot \mathbf{y})) \geq M\}$,

- $\mathcal{T} = \{(\mathbf{x}, \mathbf{y}) \in \mathcal{L} : \ p | \gcd(\mathbf{a}\cdot\mathbf{x}, \mathbf{a}\cdot\mathbf{y}) \text{ for some prime } p \le Q\}$.

Obviously $\mathcal{Q} \subseteq \mathcal{T}$ and $\mathcal{T} \setminus \mathcal{Q} \subseteq \mathcal{R} \cup S$, so that $\#\mathcal{T} - \#\mathcal{Q} \le \#\mathcal{R} + \#\mathcal{S}$. Therefore we have

$$1 - \rho_{\mathbf{a}}(M) = M^{-2m}\left(\#\mathcal{Q} + \#\mathcal{R} + \#\mathcal{S}\right) \le M^{-2m}\left(\#\mathcal{T} + \#\mathcal{R} + \#\mathcal{S}\right).$$

and

$$1 - \rho_{\mathbf{a}}(M) = M^{-2m}\left(\#\mathcal{Q} + \#\mathcal{R} + \#\mathcal{S}\right) \ge M^{-2m}\#\mathcal{T}.$$

From the above inequalities together we derive

$$|\rho_{\mathbf{a}}(M) - \zeta(2)^{-1}| \le M^{-2m}\left(|\#\mathcal{T} - (1-\zeta(2)^{-1})M^{2m}| + \#\mathcal{R} + \#\mathcal{S}\right). \quad (3)$$

For an integer $d \ge 1$, we denote by $\mathcal{U}_d(M)$ the set of all integer vectors $\mathbf{x} \in \mathbb{N}^m$ with $h(\mathbf{x}) \le M$ and $d|\mathbf{a}\cdot\mathbf{x}$, and put $U_d(M) = \#\mathcal{U}_d(M)$. Because $\gcd(a_1, \dots, a_m) = 1$, we obviously have $U_p(p) = p^{m-1}$ for any prime p. Then, for any squarefree d, by the Chinese Remainder Theorem, we conclude that $U_d(d) = d^{m-1}$, and $U_d(dK) = K^m d^{m-1}$ for any integer K.

It is also clear that for any prime p

$$U_p(M) \le \lceil M/p \rceil M^{m-1} \le M^m/p + M^{m-1}. \quad (4)$$

By the inclusion exclusion principle we have

$$M^{2m} - \#\mathcal{T} = \sum_{\substack{d \ge 1 \\ P(d) \le Q}} \mu(d) U_d(M)^2 \quad (5)$$

where μ is the Möbius function. We recall that $\mu(1) = 1$, $\mu(d) = 0$ if $d \ge 2$ is not squarefree, and $\mu(d) = (-1)^{\nu(d)}$ otherwise, where $\nu(d)$ is the number of prime divisors of d, see [5], Section 16.2. Using the bound of Theorem 4 of [7] on

$$\vartheta(x) = \sum_{p<x} \ln p, \quad (6)$$

we have

$$\prod_{p<Q} p = \exp(\vartheta(Q)) \le \exp\left(Q\left(1 + \frac{1}{2\ln Q}\right)\right) \le \exp(2Q) = \left(\frac{M}{m}\right)^{1/2},$$

since $M \ge 732m$. Thus for any squarefree d with $P(d) \le Q$, we have $d \le (M/m)^{1/2}$.

For $x > 0$, we have $(1+x)^{1/x} \le e$, and thus with $y = mx$ we have

$$\begin{aligned}(1+x)^m &= (1+x)^{y/x} \le e^y = \sum_{i\ge 0} \frac{y^i}{i!} \\ &< 1 + y + \frac{y^2}{2}\sum_{i\ge 0} y^i = 1 + y + \frac{y^2}{2(1-y)} \le 1 + 2y\end{aligned}$$

provided that $0 < x \le 2/(3m)$. Hence

$$\begin{aligned}U_d(M) &\le U_d\left(d\left\lceil\frac{M}{d}\right\rceil\right) = d^{m-1}\left(\left\lceil\frac{M}{d}\right\rceil\right)^m \\ &< d^{m-1}\left(\frac{M+d}{d}\right)^m = \frac{M^m}{d}\left(1+\frac{d}{M}\right)^m \le \frac{M^m}{d}\left(1+\frac{2md}{M}\right)\end{aligned}$$

for $M \ge 3md/2$. Similarly, $(1-x)^{1/x} \ge 1/4$ for $0 < x \le 1/2$, and thus for $0 < mx\ln 4 \le 3$ we have

$$(1-x)^m \ge e^{-mx\ln 4} = 1 - mx\ln 4 + \sum_{i\ge 2}\frac{(-mx\ln 4)^i}{i!} \ge 1 - mx\ln 4,$$

$$\begin{aligned}U_d(M) &\ge U_d\left(d\left\lfloor\frac{M}{d}\right\rfloor\right) = d^{m-1}\left(\left\lfloor\frac{M}{d}\right\rfloor\right)^m > d^{m-1}\left(\frac{M-d}{d}\right)^m \\ &= \frac{M^m}{d}\left(1-\frac{d}{M}\right)^m \ge \frac{M^m}{d}\left(1-\frac{md\ln 4}{M}\right)\end{aligned}$$

for $M \ge (dm\ln 4)/3$. We now assume that $M \ge 3md/2$, and then we have

$$\left|U_d(M) - \frac{M^m}{d}\right| \le \frac{M^m}{d}\cdot\frac{2md}{M} = 2mM^{m-1}.$$

We can estimate the difference of the squares as follows.

$$\begin{aligned}\left|U_d(M)^2 - \frac{M^{2m}}{d^2}\right| &\le \left|U_d(M) - \frac{M^m}{d}\right|\cdot\left|\frac{2M^m}{d} + 2mM^{m-1}\right| \\ &\le 2mM^{m-1}\cdot\frac{2mM^m}{d}\cdot\left(\frac{1}{m}+\frac{d}{M}\right) \\ &\le 4m^2d^{-1}M^{2m-1}\cdot\frac{2}{m} = 8md^{-1}M^{2m-1}.\end{aligned}$$

As we have seen, if d is squarefree and $P(d) \le Q$, then $d \le (M/m)^{1/2} \le 2M/(3m)$, and thus the above bounds apply.

A truncated ζ-product can be estimated as follows:

$$\left|\prod_{p>Q}\left(1-\frac{1}{p^2}\right)^{-1}-1\right| = \sum_{p|k\Rightarrow p>Q}\frac{1}{k^2}-1 < \sum_{k\ge Q}\frac{2}{k(k+1)} = \frac{2}{Q}.$$

The error in the main term for our approximation to ρ can be bounded in the following way. We use the harmonic estimate

$$\sum_{d\le x} d^{-1} \le 2\ln x$$

for $x \ge 3$ to derive

$$\begin{aligned}
\left|\#\mathcal{T} - (1-\zeta(2)^{-1})M^{2m}\right| &= \Big|\sum_{\substack{d\ge 1\\ P(d)\le Q}}\mu(d)U_d(M)^2 - \zeta(2)^{-1}M^{2m}\Big| \\
&\le \left|\sum_{\substack{d\ge 1\\ P(d)\le Q}}\mu(d)\frac{M^{2m}}{d^2} - \zeta(2)^{-1}M^{2m}\right| + \sum_{\substack{d\ge 1\\ P(d)\le Q\\ d \text{ squarefree}}}\frac{8mM^{2m-1}}{d} \\
&\le M^{2m}\left|\prod_{p\le Q}\left(1-\frac{1}{p^2}\right) - \zeta(2)^{-1}\right| + 8mM^{2m-1}\sum_{d^2\le M/m}\frac{1}{d} \\
&= \zeta(2)^{-1}M^{2m}\left|\prod_{p>Q}\left(1-\frac{1}{p^2}\right)^{-1} - 1\right| + 8mM^{2m-1}\ln(M/m) \\
&\le \zeta(2)^{-1}M^{2m}\cdot 2Q^{-1} + 8mM^{2m-1}\ln(M/m) \\
&= M^{2m}\left(2\zeta(2)^{-1}Q^{-1} + \frac{8m\ln(M/m)}{M}\right).
\end{aligned}$$

For $\#\mathcal{R}$, using (4) and the inequality $(a+b)^2 \le 2(a^2+b^2)$ we get

$$\begin{aligned}
\#\mathcal{R} &\le \sum_{Q<p<M} U_p(M)^2 \le 2 \sum_{Q<p<M} \left(\frac{M^{2m}}{p^2} + M^{2m-2} \right) \\
&\le 2M^{2m} \sum_{p>Q} \left(\frac{1}{p(p+1)} + \frac{1}{(p+1)(p+2)} \right) + 2M^{2m-2} \sum_{p<M} 1 \\
&\le 2M^{2m} \sum_{k \ge Q} \frac{1}{k(k+1)} + 2M^{2m-1} \\
&= M^{2m} \left(\frac{2}{Q} + \frac{2}{M} \right).
\end{aligned}$$

Finally, using (4) again, we find

$$\begin{aligned}
\#\mathcal{S} &\le \sum_{p \ge M} U_p(M)^2 \le M^{m-1} \sum_{p \ge M} U_p(M) \\
&= M^{m-1} \sum_{h(\mathbf{x}) \le M} \sum_{\substack{p \ge M \\ p \mid \mathbf{a}\cdot\mathbf{x}}} 1 \le M^{m-1} \cdot M^m \frac{\ln(mMN)}{\ln M},
\end{aligned}$$

since $\mathbf{a} \cdot \mathbf{x} \le mMN$, and each such number has at most $\ln(mMN)/\ln M$ many prime factors $p \ge M$.

Putting everything together and using (3), we obtain

$$|\rho_{\mathbf{a}}(M) - \zeta(2)^{-1}| \le \frac{2}{\zeta(2)Q} + \frac{8m\ln(M/m)}{M} + \frac{2}{Q} + \frac{2}{M} + \frac{\ln(mMN)}{M\ln M}.$$

It is now convenient to define $\lambda = M/m$. Using that

$$\frac{\ln(mMN)}{M\ln M} \le \frac{\ln(M^2N)}{M\ln M} = \frac{2}{M} + \frac{\ln N}{M\ln M} \le \frac{2}{M} + \frac{1}{\ln\lambda}$$

for $M \ge \ln N$, and the trivial bound $2/M \le 2/(3\lambda)$, we derive

$$\begin{aligned}
|\rho_{\mathbf{a}}(M) - \zeta(2)^{-1}| &\le \frac{8\zeta(2)^{-1}}{\ln\lambda} + \frac{8\ln\lambda}{\lambda} + \frac{8}{\ln\lambda} + \frac{2}{3\lambda} + \frac{2}{3\lambda} + \frac{1}{\ln\lambda} \\
&= \frac{8\zeta(2)^{-1}+9}{\ln\lambda} + \frac{8\ln\lambda + 4/3}{\lambda}.
\end{aligned}$$

Since $8\zeta(2)^{-1} + 9 < 13.9$ and for $\lambda = M/m \ge 9$ we have

$$\frac{8\ln\lambda + 4/3}{\lambda} \le \frac{5.1}{\ln\lambda},$$

the result now follows. □

We now show that for a small m, M must grow logarithmically with N for reasonably large success probability.

Theorem 2. *For any $m \geq 3$ and M, N with $4mM^{2m} \ln M \leq \ln N$, there is a vector $\mathbf{a} \in \mathbb{Z}^m$ of height at most N such that*

$$\rho_{\mathbf{a}}(M) \leq (1 + o(1))\, M^{-2} (\ln M)^2$$

as $M \to \infty$.

Proof. The hypothesis implies that $2M^{2m} \leq \ln N$, and we may assume that N is large enough.

Let $\mathcal{P}$ be the set of the first $T = M^{2m}$ primes p with $p > M^2$, and denote by $(\mathbf{x}, \mathbf{y}) \mapsto p_{\mathbf{x},\mathbf{y}}$ an arbitrary bijection which maps each $(\mathbf{x}, \mathbf{y}) = (x_1, \ldots, x_m, y_1, \ldots, y_m) \in \mathbb{N}^m \times \mathbb{N}^m$ of height at most M to a prime $p_{\mathbf{x},\mathbf{y}} \in \mathcal{P}$. Let $\mathcal{U}$ be the set of such pairs of vectors $(\mathbf{x}, \mathbf{y})$ with $x_1 y_2 \neq x_2 y_1$, and let $\mathcal{V}$ be the set of all other pairs.

If $(\mathbf{x}, \mathbf{y}) \in \mathcal{U}$, then obviously $0 < |x_1 y_2 - x_2 y_1| < M^2 < p_{\mathbf{x},\mathbf{y}}$, and we can find a unique integer solution $0 \leq r_{\mathbf{x},\mathbf{y}}, s_{\mathbf{x},\mathbf{y}} < p_{\mathbf{x},\mathbf{y}}$ to the system of congruences

$$\begin{aligned} x_1 r_{\mathbf{x},\mathbf{y}} + x_2 s_{\mathbf{x},\mathbf{y}} + x_3 + \cdots + x_m &\equiv 0 \bmod p_{\mathbf{x},\mathbf{y}}, \\ y_1 r_{\mathbf{x},\mathbf{y}} + y_2 s_{\mathbf{x},\mathbf{y}} + y_3 + \cdots + y_m &\equiv 0 \bmod p_{\mathbf{x},\mathbf{y}}. \end{aligned}$$

Using the Chinese Remaindering Theorem, we now define integers a_1, a_2 with

$$0 \leq a_1, a_2 < \prod_{(\mathbf{x},\mathbf{y}) \in \mathcal{U}} p_{\mathbf{x},\mathbf{y}} < \prod_{p \in \mathcal{P}} p,$$

$$\begin{aligned} a_1 &\equiv r_{\mathbf{x},\mathbf{y}} \bmod p_{\mathbf{x},\mathbf{y}}, \\ a_2 &\equiv s_{\mathbf{x},\mathbf{y}} \bmod p_{\mathbf{x},\mathbf{y}}, \end{aligned}$$

for each $(\mathbf{x}, \mathbf{y}) \in \mathcal{U}$. We denote by q the largest prime in $\mathcal{P}$. Thus q is the smallest number satisfying

$$\pi(q) \geq M^{2m} + \pi(M^2),$$

and hence $q \leq 3mM^{2m} \ln M$. We set $\mathbf{a} = (a_1, a_2, 1, \ldots, 1)$. Under the hypothesis on N, we have

$$h(\mathbf{a}) \leq \exp(\vartheta(3mM^{2m} \ln M)) \leq \exp(4mM^{2m} \ln M) \leq N,$$

where $\vartheta(x)$ is defined by (6). We also see that

$$p_{\mathbf{x},\mathbf{y}} \mid \gcd(\mathbf{a}\cdot\mathbf{x}, \mathbf{a}\cdot\mathbf{y})$$

for all $(\mathbf{x},\mathbf{y}) \in \mathcal{U}$. Therefore $\rho_{\mathbf{a}}(M) \le M^{-2m}\#\mathcal{V}$.

To estimate the cardinality of $\mathcal{V}$, we note that if $x_1y_2 = x_2y_1$ then for each pair (x_1, y_2) there are at most $\tau(x_1y_2)$ possible values for the pair (x_2, y_1), where $\tau(n)$ is the number of positive integer divisors of n. We recall that $\tau(n) = \prod_{p|n}(\alpha_p+1)$, where α_p is the multiplicity of the prime p in n, so that $\tau(ab) \le \tau(a)\tau(b)$ for any positive integers a, b, since $\alpha+\beta+1 \le (\alpha+1)(\beta+1)$ holds for any $\alpha, \beta \ge 0$. Therefore,

$$\begin{aligned}\#\mathcal{V} &\le M^{2m-4}\sum_{1\le x_1\le M}\sum_{1\le y_2\le M}\tau(x_1y_2) \le M^{2m-4}\sum_{1\le x_1\le M}\sum_{1\le y_2\le M}\tau(x_1)\tau(y_2)\\ &= M^{2m-4}\Bigg(\sum_{1\le z\le M}\tau(z)\Bigg)^2 = (1+o(1))\,M^{2m-2}\,(\ln M)^2\,,\end{aligned}$$

as $M\to\infty$ (see [5], Theorem 320), which concludes the proof. □

Of course, $\gcd(a_1,\dots,a_m)$ is trivial to determine in the example constructed in the proof. The example only shows that one has to be careful when designing a universally applicable algorithm. The gap between the "sufficient" bound $M \ge \ln N$ (ignoring m) and the "necessary" bound $M \ge (\ln N)^{1/6}$ is only polynomial. For example, we see from Theorem 2 that for $m = 3$, we have to choose M of order at least $(\ln N)^{1/6}$ to guarantee that $\rho_{\mathbf{a}}(M)$ is not too small.

3 Algorithmic Implications

Theorem 1 implies that for any $a_1,\dots,a_m$, one can compute $\gcd(a_1,\dots,a_m)$ probabilistically as the gcd of two integers of asymptotically the same bit lengths as the original data, while the result of [2] only guarantees the same for two integers of bit lengths twice more. The probability of success in both cases is, asymptotically, at least $\zeta(2)^{-1} = 6/\pi^2 = 0.6079\ldots$. Our algorithm is an attractive alternative to the m-step (deterministic) chain of computation

$$\begin{aligned}\gcd(a_1,\dots,a_m) &= \gcd(\gcd(a_1,a_2),a_3,\dots,a_m)\\ &= \gcd(\dots(\gcd(\gcd(a_1,a_2),a_3),\dots,a_m).\end{aligned}$$

For illustration, we take l-bit primes $p_1, \ldots, p_m$, $p = p_1 \cdots p_m$, and $a_i = p/p_i$ for $i \le m$. Then indeed $m - 1$ steps are necessary until the gcd, which equals 1, is found.

After $i-1$ steps, the current value of the gcd has about $(m-i)l$ bits, and the reduction of the $(m-1)l$-bit a_{i+1} modulo this gcd takes about $2l^2(m-i)(i-1)$ operations in naive arithmetic; see [3], Section 2.4. This comes to a total of about $l^2m^3/3$ operations. If one gcd of n-bit integers costs about cn^2 operations, for a constant c, which amounts to the total cost of about $cm^3/3$ operation. Thus the overall cost is about $cl^2m^3(1+c)/3$ operations.

In our algorithm, we can choose x_i and y_i of $\log(ml)$ bits (where $\log z$ is the binary logarithm of $z > 0$). The inner products together cost just over $2lm^2 \log(ml)$ operations, and the single gcd about cl^2m^2. The latter is the dominant cost, and thus our algorithm is faster by a factor of about $m/3$ than the standard one.

In other words, if $k < m/3$, maybe $k \approx \sqrt{m}$, and confidence at least $1 - \zeta(2)^{-k}$ is sufficient, then the k-fold repetition of our algorithm is faster. (In practice, one would not just repeat, but reduce the inputs modulo the gcd candidate obtained so far, and either find that it divides all of them and thus is the true gcd, or continue with the smaller values.)

When we have m rational numbers whose denominators are positive integers $p_1, \ldots, p_m$, then their sum can be expressed as a fraction with denominator

$$\operatorname{lcm}(p_1, \ldots, p_m) = p/\gcd(a_1, \ldots, a_m),$$

where $p = p_1 \cdots p_m$ and $a_i = p/p_i$ for $i \le m$, as above. Thus the advantage explained above applies to this important type of computation.

We can repeat our algorithm several times, adding each time the gcd computed (which is expected to be not much larger than the true gcd) to the list, until the same gcd is returned twice in a row. If one wants to guarantee correctness, one can then divide all elements in the list by the guessed gcd. If it divides evenly all elements, it is the true gcd.

An alternative approach would be to iteratively replace each element in the list by its remainder modulo the smallest element in the list. This will actually calculate the gcd without any gcd computation. Of course, the latter are hidden in the repeated divisions with remainder. This goes to show that our "model" of counting gcd's and ignoring all other operations is intuitively apparent in our algorithm but cannot be turned into a rigorously defined "model of computation", as long as the gcd can be calculated by the "other"

computations.

4 Remarks and Open Questions

The approach of [2] leads to an algorithm for the extended gcd; see [3] for the background on this problem. Namely, solving the the extended gcd problem for $\mathbf{a} \cdot \mathbf{x}$ and $\mathbf{a} \cdot \mathbf{y}$ we obtain a relation

$$c_1 a_1 + \ldots + c_n a_n = d$$

for some integers $c_1, \ldots, c_n, d$ with $d > 0$. Repeating this the appropriate number of times, given by (2), and choosing the relation with the smallest value of d, we solve he extended gcd problem with probability at least $1 - \delta$.

It would be very interesting to find the smallest possible rate of growth of M, as a function of N and m for which $\rho_{\mathbf{a}}(M)$ is bounded away from zero uniformly for all vectors $\mathbf{a} \in \mathbb{Z}^m$ of height at most N. In particular, it would be important to reduce the gap between the regions of parameters in Theorems 1 and 2 apply.

Finally, we recall that randomness is an expensive algorithmic resource. So it would be interesting to study $\gcd(\mathbf{a} \cdot \mathbf{x}, \mathbf{a} \cdot \mathbf{y})$ where the vectors $\mathbf{x}$, $\mathbf{y}$ are chosen from some parametric family of vectors for a random value of the parameter and thus require few random bits for their description that random independent vectors; see [1, 6] for concrete examples of such algorithms for other number theoretic problems.

References

[1] E. Bach and V. Shoup, 'Factoring polynomials using fewer random bits', *J. Symbol. Comp.*, **9** (1990), 229–239.

[2] G. Cooperman, S. Feisel, J. von zur Gathen and G. Havas, 'GCD of many integers', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **1627** (1999), 310–317.

[3] J. von zur Gathen and J. Gerhard, *Modern computer algebra*, Cambridge University Press, Cambridge, 2003.

[4] J. von zur Gathen and I. E. Shparlinski, 'GCD of random linear forms', *Proc. 15th Annual Symposium on Algorithms and Computation*, Hong Kong, 2004, Lect. Notes in Comp. Sci., Springer-Verlag, Berlin, 2004, v.3341, 455-460.

[5] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford Univ. Press, Oxford, 1979.

[6] R. Peralta and V. Shoup, 'Primality testing with fewer random bits', *Comp. Compl.*, **3** (1993), 355–367.

[7] J. B. Rosser and L. Schoenfeld, 'Approximate formulas for some functions of prime numbers', *Illinois J. Math*, **6** (1962), 64–94.