Divisors in Residue Classes, Constructively

Don Coppersmith[*]
Nick Howgrave-Graham[†]
S. V. Nagaraj[‡]

December 2, 2004

Abstract

Let r, s, n be integers satisfying $0 \le r < s < n$, $s \ge n^{\alpha}$, $\alpha > 1/4$, and $\gcd(r, s) = 1$. Lenstra showed that the number of integer divisors of n equivalent to $r \pmod{s}$ is upper bounded by $O((\alpha - 1/4)^{-2})$. We re-examine this problem; showing how to explicitly construct all such divisors and incidentally improve this bound to $O((\alpha - 1/4)^{-3/2})$.

1 Introduction

Lenstra [6] gave an existential proof of the following fact: Let r, s, n be integers satisfying $0 \le r < s < n$, $s \ge n^{\alpha}$, $\alpha > 1/4$, and $\gcd(r, s) = 1$. Then the number of divisors of n in the residue class $r \pmod{s}$ satisfies an upper bound $c(\alpha)$ depending only on α. He proves the bound $c(\alpha) = O((\alpha - 1/4)^{-2})$ by showing a general (non-constructive) result concerning weight functions of sets.

Here we construct the divisors explicitly, using techniques due to Coppersmith [2] for factoring an integer when given some knowledge of its factors, along with refinements and improved presentation due to Howgrave-Graham [4, 5].

[*]IBM Research, Yorktown Heights, NY, USA; dcopper@us.ibm.com
[†]NTRU Cryptosystems, Burlington, MA, USA; nhowgravegraham@ntru.com
[‡]Chennai, India; svn1999@eth.net

Although not explicitly stated in [2] it is shown in [1] that the techniques described in [2] can easily be used to find divisors in residue classes in polynomial time, whenever $\alpha > 1/4$ (this is done with regards to lattice attacks on RSA). We extend this observation by showing exactly which divisors may be found for $\alpha > 0$, and use an analysis of the lattice techniques to place a bound on the possible number of divisors. This analysis allows one to improve the asymptotic bound on the number of divisors given in [6] to $c(\alpha) = O((\alpha - 1/4)^{-3/2})$.

In Section 4 we outline Lenstra's original method, and show how this too can be improved from $O((\alpha - 1/4)^{-2})$ to $O((\alpha - 1/4)^{-3/2})$ by the use of similar ideas. It should be noted though, that although the two methods yield bounds which can be shown to be asymptotically similar, in practice the bounds achieved by Lenstra's methods are considerably better than the ones implied by our lattice analysis.

We start, in Section 2 by giving an overview of the lattice method and describe how one can use the LLL lattice reduction algorithm (see [7]) to explicitly construct the required divisors. The proofs in this section are deliberately vague, and it is left until Section 3 to give a completely rigorous proof of our result.

In Section 5 we compare our work with the efficient technique described in [8] and [9], which works for all $\alpha \geq 0.3$, when all the divisors of n are congruent to 1 modulo s.

In Section 6 we list some of the many interesting questions that still remain open regarding this problem.

2 An overview of the method

In this section we start by giving an outline of the results and proofs necessary for our result, and then show how to explicitly search for the required divisors in residue classes. For more details and a complete analysis please refer to Section 3.

We are concerned with divisors of n of the form $(sx + r)$, and therefore should start by giving the following trivial result.

Lemma 2.1 *Given s, r, n and α with $s = n^\alpha$ and $\alpha > 1/2$, there are at most two positive divisors of n of the form $(sx + r)$.*

Proof. The divisors of n of the form $(sx + r)$ are paired with those of the form $(sy + r')$ where $r' = n/r \pmod{s}$, $0 < r' < s$. If $s > n^{1/2}$ and $x \geq 1$ then its corresponding factor must be $s \times 0 + r'$, and so there can be only one divisor with $x \geq 1$, and one with $x = 0$. This also holds when $r = r'$. $\square$

The rest of the paper is based around the following theorem and corollary.

Theorem 2.1 *Given p and n with $p = n^{\alpha}$, all x such that $(p + x)$ divides n and $|x| < n^{\gamma}$ can be found in polynomial time whenever*

$$\gamma h(h-1) - 2u\alpha h + u(u+1) \quad < \quad 0,$$

for some integers $h > u > 0$. The largest value of γ for which this can hold is $\alpha^2 - \epsilon$.

Proof. We set $X = n^{\gamma}$. For the given integers $h > u > 0$ form the $h \times h$ matrix $M(h, u, X)$ with rows corresponding to the polynomials

$$q_i(x) \quad = \quad \begin{cases} n^{u-i}(p+x)^i & 0 \leq i \leq u, \\ x^{i-u}(p+x)^u & u < i < h. \end{cases}$$

For example

$$M(4,2,X) \quad = \quad \begin{pmatrix} n^2 & 0 & 0 & 0 \\ np & nX & 0 & 0 \\ p^2 & 2pX & X^2 & 0 \\ 0 & p^2X & 2pX^2 & X^3 \end{pmatrix}$$

Now apply the LLL lattice reduction algorithm to the rows of this matrix to find a small row b_1, and associate with this small lattice vector the polynomial

$$b_1(x) \quad = \quad b_1 \cdot \left(1, \left(\frac{x}{X}\right), \left(\frac{x}{X}\right)^2, \left(\frac{x}{X}\right)^3\right),$$

where $v_1 \cdot v_2$ denotes the vector dot product. Notice that the polynomials associated with the rows of $M(h, u, X)$ are all zero modulo $(p + x_0)^u$ when evaluated at $x = x_0$ if $(p + x_0)|n$. This means that $b_1(x)$ also has this property since it is an integer linear combination of these polynomials.

From the LLL bound on the small vector b_1 we will then have, for all $|x| < X$, that

$$|b_1(x)| \quad < \quad cn^{u(u+1)/2h} X^{(h-1)/2}$$

for some small multiple c which we shall choose to ignore. The right hand side is less than $n^{u\alpha}$ whenever

$$X \quad < \quad n^{\frac{u(2\alpha h-u-1)}{h(h-1)}}.$$

or

$$\gamma h(h-1) - 2u\alpha h + u(u+1) \quad < \quad 0.$$

If $b_1(x)$ is such that $b_1(x_0) = 0 \pmod{(p+x_0)^u}$ for all x_0 such that $(p+x_0)|n$, and also $b_1(x_0) < n^{u\alpha}$ for all $|x_0| < X$, then any $|x_0| < X$ such that $(p+x_0)|n$ must be a root of $b_1(x)$ over the integers, and hence may be found in polynomial time.

For a given h the choice of u that maximizes γ is $u = \alpha h - 1/2$, which means that $\lim_{h\to\infty} \gamma = \alpha^2$. $\square$

One can readily extend the result to the following.

Corollary 2.1 *All x such that $(sx+r)$ divides n where $s = n^\alpha$ and $n^\beta < |x| < n^\gamma$ can be found whenever*

$$\gamma h(h-1) - 2u(\alpha+\beta)h + u(u+1) \quad < \quad 0,$$

for any $h > u > 0$, and the largest value of γ for which this can hold is $(\alpha+\beta)^2 - \epsilon$.

Proof. We use the fact that $|x| > n^\beta$ to put a lower bound on the size of $(sx+r)$. If $s' = s^{-1} \bmod n$, then following are both divisible by $(sx+r)$:

$$n$$

$$s'(sx+r) \quad = \quad x + r'' \pmod{n}$$

This implies we form the matrix as before with $p = r''$ and now all the rows are multiplies of $(sx+r)^u > n^{(\alpha+\beta)u}$, and thus so is $b_1(x)$. The remaining analysis follows that shown before.

The best choice of u is $(\alpha+\beta)h - 1/2$, implying $\lim_{h\to\infty}\gamma = (\alpha+\beta)^2$. $\square$

Figure 1 below represents the space of possible divisors of the given integer n, which are less than $\sqrt{n}$. A divisor $(sx+r)$ corresponds to a point $(\log_n s, \log_n x)$, which means that all such divisors lie under the line drawn from $(0, 1/2)$ to $(1/2, 0)$, and also that all the divisors we are searching for lie in a vertical line at $(\alpha, \log_n x)$. Such a line is drawn for $\alpha = 0.29$. It will be useful to refer to this diagram in the following discussion.

For given n, s, r we may use Corollary 2.1 to find some of the divisors $sx+r$ of n, for any $\alpha = \log_n s > 0$. To see exactly which ones these are, notice that if we set $X = n^\gamma$, and reduce the relevant lattice, then (by choosing a sufficiently large h) we will find all divisors with $n^{\sqrt{\gamma}-\alpha} < |x| < X = n^\gamma$. Clearly for this range to exist (and thus for the Corollary to be useful) we require that

$$\sqrt{\gamma} - \gamma \quad \leq \quad \alpha,$$

which is the curved line drawn in Figure 1. The Corollary will therefore help (to some degree) to find the divisors anywhere in the lower region of Figure 1, defined by this curve for $0 < \alpha \leq 1/4$, and the line $\gamma = 1/2 - \alpha$ for $1/4 < \alpha \leq 1/2$.

For a given $\alpha = \log_n s > 1/4$, if we wish to find all the possible divisors $sx + r$ less than $\sqrt{n}$, then we must let x range between 1 and $n^{1/2-\alpha}$, and so we must use the Corollary repeatedly on subsections of this interval[1]. As we will see, we may decide to use relatively small values of h, in the interest of increasing the speed of our method or in bounding the number of possible divisors. The effect of decreasing h will be to decrease the size of the intervals, and thus increase the number of them we need consider. The reason that h has a rôle to play in bounding the number of divisors is that the degree of the polynomial one obtains, after the lattice reduction, is $h-1$, and we know that all of the relevant divisors of n in this interval must be factors of this polynomial (so clearly there can be at most $h-1$ of them).

It should also be mentioned at this point, that since the lattice techniques are concerned with the absolute value of x, we do end up finding the divisors, $s(-x) + r = -(sx - r)$ as well by this process, and so these are counted by

[1]We should also remember that there may a divisor of n with $x = 0$, i.e. r itself.

$h-1$ too. It is not presently known how to place a bound on the number of divisors of the form $sx+r$ for just $x>0$ using these lattice techniques.

As an example of this, for $\alpha = 0.29$ it turns out to be optimal (with respect to bounding the number of divisors) to choose 7 intervals. Working from the bottom one first these are parametrized by

$$(h_i, u_i) \quad = \quad (5,1),(8,2),(9,3),(11,4),(13,5),(14,6)$$

which implies that

$$\log_n X_i = \gamma_i \quad = \quad 0, 0.04, 0.08, 0.11, 0.14, 0.17, 0.19, 0.21$$

are the values defining the partitioning of the interval $[0, 0.21]$ (these subintervals are also indicated in Figure 1). The total number of divisors of the form $sx+r$ or $sx-r$ for $\alpha = 0.29$ is thus twice (because we must count the divisors more than $\sqrt{n}$ too) the sum of the $h_i - 1$ plus two (to count the fact that 1 and n may also equal r mod s); namely 132 in this example.

In general to work out the optimal way to split the intervals, one may assume one wants m intervals, and then exhaustively search[2] the possible h_i and u_i, where $\beta_0 = 0$ and

$$\beta_i = \gamma_{i-1} = \frac{2u_i(\alpha + \beta_{i-1})h_i - u_i(u_i+1)}{h_i(h_i-1)}$$

Notice that these interval partitions are linear in α. With m intervals we require that $\beta_m > 1/2 - \alpha$, which we may solve, to determine the least α with at most $2(\sum(h_i - 1) + 1)$ divisors $sx \pm r$.

Table 5.2 in Section 5 indicates the α at which increasing the number of intervals becomes preferable to increasing the values of h in any interval.

[2]This search space can be considerably reduced by only searching near the optimal values shown in Lemma 2.2, when an estimate of α is known.

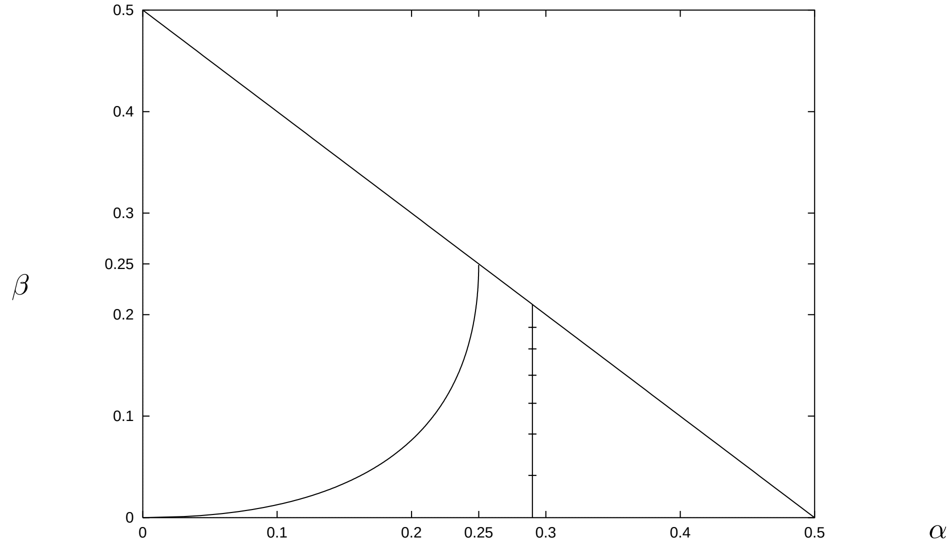

Figure 1: *A description of the divisors one can find*

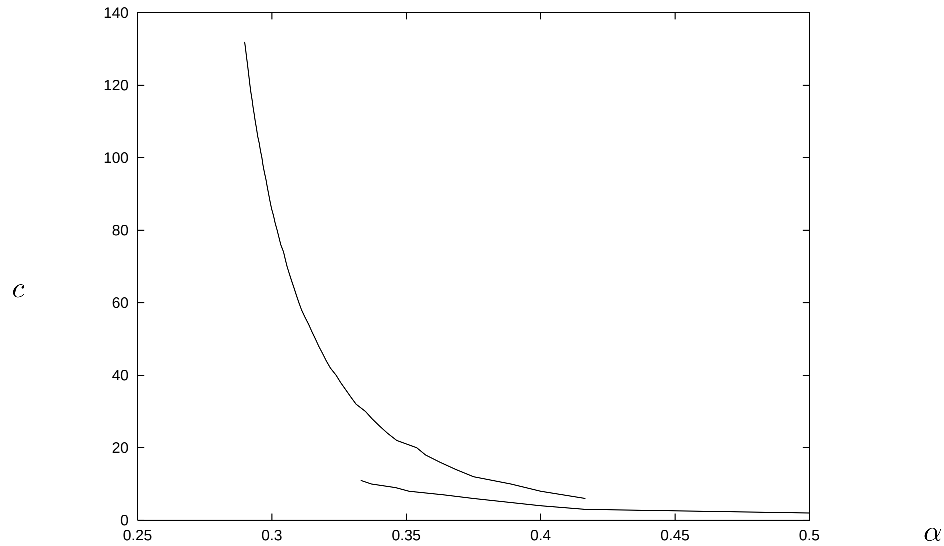

Figure 2: *The bounds on the number of divisors*

The upper curve in Figure 2 above represents the bound on the number of divisors achieved by this process for $\alpha \geq 0.29$. The lower curve is the presently best known bounds for $\alpha \geq 1/3$; which can be seen to be considerably better (ending up by a factor of slightly more than 2). It would be an interesting exercise to see if one could align these two sets of results more closely.

To analyze the asymptotic behavior of the upper curve in Figure 2, we can do the following analysis.

Lemma 2.2 *The number of divisors of n of the form $(sx+r)$ less than $\sqrt{n}$ is approximately bounded by*

$$c(\alpha) \quad \leq \quad \frac{\pi\alpha}{(\alpha - 1/4)^{3/2}}.$$

"Proof". Starting with $\beta = 0$, and increasing to $\beta = 1/2 - \alpha$, we choose h and u to imply a γ which minimizes the density of divisors $(h-1)/(\gamma - \beta)$. These values are

$$\begin{aligned} h &= \left\lceil \frac{2\alpha}{(\alpha+\beta)^2 - \beta} \right\rceil, \\ u &= \lfloor (\alpha+\beta)h \rfloor, \\ \gamma &= \frac{2(\alpha+\beta)uh - u(u+1)}{h(h-1)}. \end{aligned}$$

The density of divisors then satisfies

$$\frac{h-1}{\gamma - \beta} \quad < \quad \frac{4\alpha}{((\alpha+\beta)^2 - \beta)^2}.$$

Since this an increasing function for all $\beta < 1/2 - \alpha$ we have that

$$h - 1 < (\gamma - \beta)\frac{4\alpha}{((\alpha+\beta)^2 - \beta)^2} < \int_{v=\beta}^{\gamma} \frac{4\alpha}{((\alpha+v)^2 - v)^2} dv.$$

This means that

$$\begin{aligned} \sum h - 1 \quad &< \quad \int_0^{1/2-\alpha} \frac{4\alpha}{((\alpha+v)^2 - v)^2} dv \\ &< \quad \frac{\pi\alpha}{(\alpha - 1/4)^{3/2}}. \end{aligned}$$

□

In the next section we go through the fine details of what we have alluded to in the above "proof". This mainly means tightening the analysis, and being specific about all the required integers values.

3 The construction

Lemma 3.1 *Assume given integers $h > u > 0$ and reals α, β, γ satisfying*

$$\begin{gathered} 0 < \alpha < 1 \\ 0 \le \beta < \gamma \le 1 - \alpha \\ u(u+1) + \gamma h(h-1) - 2(\alpha+\beta)uh < 0. \end{gathered}$$

Then there exists an effectively computable integer $n_0 > 0$ such that for all integers $0 < r < s < n$ with

$$\begin{gathered} n > n_0 \\ s \ge n^\alpha \\ \gcd(r,s) = \gcd(s,n) = 1, \end{gathered}$$

the number of pairs of integers (d, x) satisfying

$$\begin{gathered} d | n \\ d = sx + r \\ n^\beta \le x \le n^\gamma \end{gathered}$$

is bounded above by $h - 1$. We give a procedure to find these divisors in time polynomial in $(u, h, \log n)$.

Proof.

We will calculate n_0 later.

For a given instance (n, r, s) of our problem, because $\gcd(n, s) = 1$, we can find an integer $m = s^{-1}r \pmod n$, using the extended Euclidean algorithm.

Consider the polynomials

$$p_i(x) = \begin{cases} n^{u-i}(x+m)^i & 0 \le i \le u \\ x^{i-u}(x+m)^u & u < i < h \end{cases}$$

If $d_0 = sx_0 + r$ is a divisor of n in the desired range, then each $p_i(x_0)$ is a multiple of d_0^u. This follows because $x_0 + m = s^{-1}d_0 \pmod n$.

Any integer linear combination of the p_i yields a polynomial which evaluates, at x_0, to a multiple of d_0^u.

Let $X = \lfloor n^\gamma \rfloor$ be the upper bound on the values of $|x|$ under consideration.

We build an $h \times h$ matrix M whose columns correspond to powers of x, and whose rows correspond to the polynomials p_i, in the sense that m_{ij} is X^j times the coefficient of x^j in the polynomial $p_i(x)$. M is lower triangular, so its determinant is given by the product of its diagonal elements, namely $\det(M) = n^{u(u+1)/2} X^{h(h-1)/2}$.

We consider the rows of M to be the basis of an integer lattice. We apply the lattice basis reduction algorithm from [7] to find a relatively short element of this lattice: a row vector v whose L_2 norm satisfies

$$\parallel v \parallel = \left(\sum_j v_j^2 \right)^{1/2} \leq 2^{(h-1)/4} (\det(M))^{1/h}.$$

Interpreting this row as a polynomial, which is to be evaluated at the point x_0, we compute:

$$|v(x_0)| \leq \sqrt{h} \parallel v \parallel \leq 2^{(h-1)/4} \sqrt{h} \left(n^{u(u+1)/2} X^{h(h-1)/2} \right)^{1/h}.$$

The hypotheses imply

$$u(u+1) + \gamma h(h-1) - 2(\alpha + \beta) uh = -\epsilon < 0.$$

We select

$$n_0 = 1 + \left\lfloor \left(2^{(h-1)/4} \sqrt{h} \right)^{2h/\epsilon} \right\rfloor.$$

Then we have

$$\begin{array}{rcl}
|v(x_0)| & \leq & \left(2^{(h-1)/4} \sqrt{h} \right) \left(n^{u(u+1)/2} X^{h(h-1)/2} \right)^{1/h} \\
& < & (n_0^{\epsilon/2h}) \left(n^{u(u+1)/2} X^{h(h-1)/2} \right)^{1/h} \\
& < & \left(n^{\epsilon} n^{u(u+1)} X^{h(h-1)} \right)^{1/2h} \\
& \leq & \left(n^{\epsilon + u(u+1) + \gamma h(h-1)} \right)^{1/2h} \\
& = & \left(n^{2(\alpha+\beta)uh} \right)^{1/2h} \\
& = & n^{(\alpha+\beta)u} \\
& < & d_0^u.
\end{array}$$

The last inequality follows from $d_0 > x_0 s \geq n^{\alpha+\beta}$. Since $v(x_0)$ is a multiple of d_0^u, and we have just seen $|v(x_0)| < d_0^u$, we conclude $v(x_0) = 0$.

Thus for all x_0 in the range $n^\beta \le x_0 \le n^\gamma$ we know that $v(x_0) = 0$, so that x_0 is a root of v. Then $h - 1 = deg(v)$ is an upper bound on the number of divisors in that range. Further, we can compute these divisors by building the matrix, doing lattice basis reduction, and solving a univariate polynomial over the integers, all of which are polynomial-time operations.

$\square$

Lemma 3.2 *Given $\alpha > 1/4$ there is an integer $n_0 > 0$ such that for all integers $n > n_0$ and $s > n^\alpha$ and $0 < r < s < n$ with* $\gcd(r, s) = \gcd(s, n) = 1$*, the number of divisors d of n with $d \le \sqrt{n}$ and $d \equiv r \pmod{s}$ is bounded above by*

$$1 + \frac{\pi\alpha}{(\alpha - 1/4)^{3/2}} + \frac{2\alpha}{\alpha - 1/4}.$$

We give a procedure to find these divisors in time polynomial in $(\log n, (\alpha - 1/4)^{-1})$.

Corollary 3.1 *Given $\alpha > 1/4$ there is an integer $n_0 > 0$ such that for all integers $n > n_0$ and $s > n^\alpha$ and $0 < r < s < n$ with* $\gcd(r, s) = \gcd(s, n) = 1$*, the number of divisors d of n with $d \equiv r \pmod{s}$ is bounded above by*

$$2 + \frac{2\pi\alpha}{(\alpha - 1/4)^{3/2}} + \frac{4\alpha}{\alpha - 1/4}.$$

We give a procedure to find these divisors in time polynomial in $(\log n, (\alpha - 1/4)^{-1})$.

Proof. (of Corollary 3.1) Apply Lemma 3.2 twice, the second time with $r' \equiv n/r \pmod{s}$. Divisors d of n larger than $\sqrt{n}$ and equivalent to $r \pmod{s}$ correspond to divisors d' of n smaller than $\sqrt{n}$ and equivalent to $r' \pmod{s}$ by $dd' = n$. $\square$

Proof. (of Lemma 3.2). The divisors $d = sx + r$ with $n^0 \le x \le n^{1/2-\alpha}$ include all those we are interested in, with the possible exception of $d = r$ corresponding to $x = 0 < n^0$. This is the first "1" in the formula.

The closed interval $I = [0, 1/2 - \alpha]$ contains $\log_n x$. We will divide I into sub-intervals $I_j = [\beta_j, \gamma_j)$, $j = 1, 2, \ldots, J$, with $\beta_1 = 0$, $\gamma_j = \beta_{j+1}$, and $\gamma_J > 1/2 - \alpha$. We will provide u_j, h_j for each interval, satisfying the conditions of Lemma 3.1. At most $h_j - 1$ values x lie in each sub-interval I_j, and the sum $\sum(h_j - 1)$ will give the desired bound.

For fixed α and for each $\beta = \beta_j$ in turn, we choose parameters u, γ, h so as to minimize the density of roots in the neighborhood: with at most $h-1$ divisors in the range $[n^{\alpha+\beta}, n^{\alpha+\gamma})$, we strive to minimize $(h-1)/(\gamma-\beta)$.

To this end, we set

$$\begin{array}{c} h = \left\lceil \frac{2\alpha}{(\alpha+\beta)^2-\beta} \right\rceil \\ u = \lfloor (\alpha+\beta)h \rfloor \end{array}$$

so that

$$\begin{array}{c} \frac{2\alpha}{(\alpha+\beta)^2-\beta} \le h < \frac{2\alpha}{(\alpha+\beta)^2-\beta} + 1 \\ (\alpha+\beta)h - 1 < u \le (\alpha+\beta)h. \end{array}$$

We also select γ in the range

$$\beta < \gamma < \gamma_{max} = \frac{2(\alpha+\beta)uh - u(u+1)}{h(h-1)},$$

so that the hypothesis of Lemma 3.1 is satisfied.

For fixed α, β, h, with u at either of its extrema we have

$$\gamma_{max} \ge \frac{(\alpha+\beta)^2h^2 - (\alpha+\beta)h}{h(h-1)} = \frac{(\alpha+\beta)^2h - (\alpha+\beta)}{h-1}$$

and the same holds for u in the interior of its allowed range, by convexity. Then

$$\gamma_{max} - \beta \ge \frac{((\alpha+\beta)^2-\beta)h - \alpha}{h-1}.$$

The numerator of this expression is minimized when h is minimized, at $h = 2\alpha/((\alpha+\beta)^2-\beta)$, yielding

$$numerator \ge \alpha.$$

The denominator is maximized when h is maximized, at

$$h \quad = \quad 2\alpha/((\alpha+\beta)^2-\beta) + 1,$$

yielding

$$denominator \quad < \quad \frac{2\alpha}{(\alpha+\beta)^2-\beta}.$$

We conclude

$$\begin{aligned} \gamma_{max} - \beta \quad &> \quad \frac{\alpha}{2\alpha/((\alpha+\beta)^2-\beta)} \\ &= \quad \frac{1}{2}\left[(\alpha+\beta)^2 - \beta\right], \end{aligned}$$

and the density satisfies

$$\frac{h-1}{\gamma_{max}-\beta} \quad < \quad \frac{4\alpha}{((\alpha+\beta)^2-\beta)^2}.$$

Notice that the density function $f(\beta) = \frac{4\alpha}{((\alpha+\beta)^2-\beta)^2}$ is an increasing function of β for $\beta < 1/2-\alpha$, so that

$$h-1 < (\gamma_{max}-\beta)f(\beta) < \int_\beta^{\gamma_{max}} f(v)dv.$$

So we can select γ slightly less than γ_{max} so that we still have

$$h-1 < \int_\beta^\gamma f(v)dv.$$

Let u_j, h_j, γ_j be defined by (u, h, γ), and let the value n_0 from Lemma 3.1 be known as $n_{0,j}$. Lemma 3.1 then tells us that the number of divisors $d = xs + r$ with $\beta_j \le \log_n x < \gamma_j$ is at most $h_j - 1$, as long as $n > n_{0,j}$.

Continue to produce intervals $[\beta_j, \gamma_j)$ until $\gamma_J > 1/2 - \alpha$. Then upper bound h_J by its largest possible value,

$$h_J = \left\lceil \frac{2\alpha}{(\alpha+\beta_J)^2-\beta_J} \right\rceil \le \left\lceil \frac{2\alpha}{((\alpha+(1/2-\alpha))^2-(1/2-\alpha)} \right\rceil < \frac{2\alpha}{\alpha-1/4}+1$$

$$h_J - 1 < \frac{2\alpha}{\alpha-1/4}$$

The total number of divisors is now bounded by

$$\begin{aligned}
1+\sum_{j=1}^{J-1}(h_j-1)+(h_J-1) &\le 1+\sum_{j=1}^{J-1}\int_{\beta_j}^{\gamma_j} f(v)dv+\tfrac{2\alpha}{\alpha-1/4} \\
&< 1+\int_0^{1/2-\alpha} f(v)dv+\tfrac{2\alpha}{\alpha-1/4} \\
&= 1+\int_0^{1/2-\alpha} \tfrac{4\alpha dv}{((\alpha+v)^2-v)^2}+\tfrac{2\alpha}{\alpha-1/4} \\
&= 1+4\alpha\int_{-1/2+\alpha}^0 \tfrac{dx}{((x+1/2)^2-(x+1/2-\alpha))^2} \\
&\quad +\tfrac{2\alpha}{\alpha-1/4};
\end{aligned}$$

the latter equation coming from the substitution $v = x + 1/2 - \alpha$;

$$\begin{aligned}
&= 1+4\alpha\int_{-1/2+\alpha}^0 \tfrac{dx}{(x^2+(\alpha-1/4))^2}+\tfrac{2\alpha}{\alpha-1/4} \\
&< 1+4\alpha\int_{-\infty}^0 \tfrac{dx}{(x^2+(\alpha-1/4))^2}+\tfrac{2\alpha}{\alpha-1/4} \\
&< 1+4\alpha\tfrac{\pi/4}{(\alpha-1/4)^{3/2}}+\tfrac{2\alpha}{\alpha-1/4} \\
&< 1+\tfrac{\pi\alpha}{(\alpha-1/4)^{3/2}}+\tfrac{2\alpha}{\alpha-1/4}.
\end{aligned}$$

This estimate holds for all $n > \max n_{0,j}$, so we set $n_0 = \max n_{0,j}$, and we are done. □

4 Lenstra's method

Our bound on the density of divisors allows relatively more divisors near the middle, $d \approx n^{1/2}$, and fewer near the ends, $d \approx n^0, n^1$. By contrast, Lenstra's original proof covered the unit interval with intervals of fixed length ϵ, and proved a uniform bound on the number of roots whose log (base n) lie in any ϵ-interval. His result was $O((\alpha - 1/4)^{-2})$ roots overall. If one follows Lenstra's proof but instead covers the unit interval with intervals with variable length ϵ and computes independently the bounds on the number of roots in each interval, one gets the same $O((\alpha - 1/4)^{-3/2})$ bound as the present approach. We outline here this improvement, borrowing liberally from Lenstra's paper.

For a positive integer k put

$$V(k) = \{p^t : p \text{ prime}, t \in \mathbf{Z}, t \geq 1, p^t \text{ divides } k\}$$

and define a weight w on each set $V(k)$ by $w(\{p^t\}) = \log_n p$. It follows that $w(V(k)) = \log_n k$.

Choose parameters β, ϵ with $\alpha \leq \beta$ and $\beta + \epsilon \leq 1$. (Warning: Lenstra's β corresponds to our $\beta + \alpha$.) Set $m = |\mathbf{D}_\beta|$ where

$$\mathbf{D}_\beta = \{d : d|n, d \equiv r \pmod{s}, \beta \log n \leq \log d < (\beta + \epsilon) \log n\}.$$

Set $D = V(d)$.

Consider $d, d' \in \mathbf{D}_\beta$ and the corresponding sets $D = V(d), D' = V(d')$. We have $\beta \leq w(D), w(D') < \beta + \epsilon$. In particular $w(D)$ and $w(D')$ differ by less than ϵ. Subtracting $(D \cap D')$ we find that $w(D - D')$ and $w(D' - D)$ also differ by less than ϵ. The larger is at least $\alpha = \log_n s$, so the smaller is strictly greater than $\alpha - \epsilon$. (Essentially this is using the fact that $\gcd(d, d') \leq |x - x'|$ when $d = sx + r, d' = sx' + r$). The symmetric difference $D \Delta D'$ satisfies $w(D \Delta D') > 2\alpha - \epsilon$. Summing over all unordered pairs of $d_i \in \mathbf{D}_\beta$ we have

$$\sum_{1 \leq i < j \leq m} w(D_i \Delta D_j) > \binom{m}{2}(2\alpha - \epsilon).$$

For each prime power $p^t|n$, let x denote the corresponding multiset element, and set $m_x = \sharp\{i : x \in D_i\}$. We have

$$\sum_{1 \leq i < j \leq m} w(D_i \Delta D_j) = \sum_x (m_x)(m - m_x) w(\{x\})$$

Set

$$\tau = \sum_x \frac{m_x}{m} w(\{x\}) = \frac{1}{m} \sum_i w(D_i)$$

so that

$$\beta \leq \tau < \beta + \epsilon.$$

By convexity[3] of the function $t(m-t)$ we find

$$\sum_x (m_x)(m - m_x) w(\{x\}) \leq (m\tau)(m(1-\tau)),$$

which is the fundamental equation which allows us to treat the intervals separately (rather than considering the (constant) bound of $m^2/4$).

Combining, we see

$$\binom{m}{2}(2\alpha - \epsilon) < m^2 \tau(1-\tau)$$

$$(m-1)(2\alpha - \epsilon) < 2m\tau(1-\tau)$$

$$1 - \frac{1}{m} = \frac{m-1}{m} < \frac{\tau(1-\tau)}{\alpha - (\epsilon/2)}$$

$$m < \frac{\alpha}{\alpha + \tau^2 - \tau - \frac{\epsilon}{2}}$$

Let

$$\epsilon = \alpha + \tau^2 - \tau = (\alpha - \frac{1}{4}) + (\tau - \frac{1}{2})^2 > 0.$$

Then we find

$$m < \frac{2\alpha}{\alpha + \tau^2 - \tau}$$

$$\frac{m}{\epsilon} < \frac{2\alpha}{(\alpha + \tau^2 - \tau)^2}$$

As before, the latter fraction represents a density of roots. This density corresponds to half of our $f(\tau - \alpha)$. We then integrate from 0 to 1, taking care of details in a manner similar to the previous section, which yields an upper bound of about

$$\frac{\pi\alpha}{(\alpha - \frac{1}{4})^{3/2}}$$

for the total number of divisors.

[3]This is covered in more detail in the Appendix A.

5 Results

With respect to bounding the number of divisors, the previously best known results for $\alpha \geq 1/3$ are as follows:

Table 5.1 *The best known bounds for given $\alpha \geq 1/3$.*

α *(approx.)*	1/2 (.5)	2/5 (.4)	3/8 (.375)	4/11 (.364)	13/37 (.351)	9/26 (.346)	31/92 (.337)	1/3 (.333)
$c(\alpha)$	2	4	6	7	8	9	10	11

Our results do not compare well with the above; mainly, it is thought, because we are counting the number of divisors of the form $sx-r$ as well. Out of interest the following table indicates the α at which it becomes preferable to increase the number of intervals, rather than increase the value of h in any one of them, together with the bound on the number of divisors at this α.

Table 5.2 *The first α for which it is best to increase the number of intervals.*

# *intervals*	α	*(approx.)*	$c(\alpha)$
1	5/12	(0.417)	6
2	7/18	(0.389)	10
3	23/65	(0.354)	20
4	55/166	(0.331)	32
5	6799/21420	(0.317)	48
6	6233/20440	(0.305)	72
7	24159/81550	(0.296)	100

6 Conclusions

One reason that the lattice bounds are worse is that they actually count the divisors in residue classes of the form $sx - r$ as well. It would be nice if one could remove this necessity, and further align our result with Lenstra's.

It would also be interesting to know if the divisors indicated by Figure 1, completely describe those that can be found in polynomial time. If such a statement could be shown to be true, then it poses the problem of how hard the remaining divisors are to find. To find the divisors in the top left of this diagram is clearly equivalent to the hardest factorization problem (since one may exhaustively search for small enough r and s), but are there a series of complexity classes that lead up to this?

In contrast to the given problem, is that of actually constructing numbers n with a given number of divisors in the same residue class. Cohen (see [3]) has shown that there are an infinitely many numbers with 6 divisors in the same residue class, i.e. those of the form $n = (2x+1)(x^2+1)(x^2+x+1)(2x^2-x+1)(2x^2+x+1)$ with $r = 1$ and $s = (2x+1)(x^2+1)-1$. Since $s > n^{1/3}$ for all $x > 5$ we have that $c(1/3) \geq 6$. Comparing this with the known upper bound of 11 divisors, shows there is plenty of work needed in aligning these two sets of results.

The techniques of Section 3 worked out the optimal parameters for bounding the number of divisors, not for speed of finding them. In order to promote the use of this algorithm in finding divisors in residue classes in practice, it would be nice to suggest good practical choices of parameters for any α. However, choosing semi-optimal parameters relies on having a good estimate of lattice reduction running times. At present we leave this as an open question.

7 Acknowledgments

We thank Carl Pomerance for his encouragement, and for interesting discussions regarding the links of this work with primality proving. The second author would like to acknowledge both the University of Bath, UK, and IBM, Yorktown Heights, where most of this work was done. Similarly the third author would like to acknowledge the IBM Tokyo Research Lab, and Professor R. Balasubramanian.

References

[1] D. Boneh, G. Durfee, Y. Frankel, "An attack on RSA given a fraction of the private key bits" *Proceedings of Asiacrypt 98*, Springer LNCS volume 1514, pages 25-34.

[2] D. Coppersmith, "Finding a small root of a bivariate integer equation; factoring with high bits known." *Proceedings of Eurocrypt 96*, Springer LNCS volume 1070, pages 178-189.

[3] H. Cohen, "Diviseurs appartenant à une même classe résiduelle", *Seminar on number theory, 1982-83*, University of Bordeaux I, Talence, Exp. No. 16, 12 pp., 1982-83.

[4] N. A. Howgrave-Graham, "Finding small solutions of univariate modular equations revisited." Pages 131-142 of: Cryptography and Coding. LNCS, vol 1355. Springer-Verlag, 1997.

[5] N. A. Howgrave-Graham, "Computational mathematics inspired by RSA." Ph.D. thesis, University of Bath, UK. 1999.

[6] H. W. Lenstra, Jr., "Divisors in Residue Classes," *Mathematics of Computation*, volume 42, number 165, January 1984, pages 331-340.

[7] A. K. Lenstra, H. W. Lenstra and L. Lovasz, "Factoring Polynomials with Integer Coefficients," Matematische Annalen **261** (1982), 513–534.

[8] C. Pomerance, S. Konyagin, "On primes recognizable in deterministic polynomial time", in "The Mathematics of Paul Erdös", Eds.: R.L. Graham, J. Nesetril, 1996. ISBN 3-540-61032-4.

[9] R. Crandall, C. Pomerance, "Prime numbers: a computational perspective", Springer-Verlag, New York, NY, ISBN 0-387-94777-9. 2001.

[10] V. Shoup, "NTL: A Library for doing Number Theory (version 4.0a)", `www.shoup.net`

A A proof of convexity

In Section 4 we required the following result with respect to the convexity of the function $t(m-t)$.

Theorem A.1 *For any set of real numbers $x_1, \ldots, x_n$, with associated (real) positive weights $w_1, \ldots, w_n$ we have that*

$$\left(\sum_{i=1}^{n} w_i\right)\left(\sum_{i=1}^{n} x_i(m-x_i)w_i\right) \quad \leq \quad \left(\sum_{i=1}^{n} x_i w_i\right)\left(\sum_{i=1}^{n}(m-x_i)w_i\right)$$

Proof. Let δ be the righthand side minus the lefthand side, i.e.

$$\delta \quad = \quad \left(\sum_{i=1}^{n} x_i w_i\right)\left(\sum_{i=1}^{n}(m-x_i)w_i\right) - \left(\sum_{i=1}^{n} w_i\right)\left(\sum_{i=1}^{n} x_i(m-x_i)w_i\right),$$

By introducing a second summation variable j, and bringing both summation to the front we have

$$\delta = \sum_{i=1}^{n}\sum_{j=1}^{n} w_i w_j (x_i(m - x_j) - x_i(m - x_i))$$

Note that the (polynomial) coefficients of each of the w_i^2 terms disappear, so there are only $n(n-1)/2$ unique $w_i w_j$ terms remaining. If we now performing our grouping by these terms, then we have:

$$\begin{aligned}
\delta &= \sum_{i=1}^{n}\sum_{j=1}^{i-1} w_i w_j (x_i(m - x_j) - x_i(m - x_i) + x_j(m - x_i) - x_j(m - x_j)) \\
&= \sum_{i=1}^{n}\sum_{j=1}^{i-1} w_i w_j (x_i^2 - 2x_i x_j + x_j^2) \\
&= \sum_{i=1}^{n}\sum_{j=1}^{i-1} w_i w_j (x_i - x_j)^2 \\
&\geq 0
\end{aligned}$$

□