Date: 2003.09.28. Permanent ID of this document: b4795a4f12863c26de5b7afe9296ffd8. Refereed. Will be printed in *Primes and misdemeanours: lectures in honour of the sixtieth birthday of Hugh Cowie Williams*, 2004.

Doubly focused enumeration of locally square polynomial values

Daniel J. Bernstein
Department of Mathematics, Statistics, and Computer Science (M/C 249)
The University of Illinois at Chicago
Chicago, IL 60607–7045
djb@cr.yp.to

Abstract. Let f be a nonconstant squarefree polynomial. Which of the values $f(c+1), f(c+2), \ldots, f(c+H)$ are locally square at all small primes? This paper presents an algorithm that answers this question in time $H/M^{2+o(1)}$ for an average small c as $H \to \infty$, where $M = H^{1/\log_2 \log H}$. In contrast, the usual method takes time $H/M^{1+o(1)}$. This paper also presents the results of two record-setting computations: an enumeration of locally square integers up to $24 \cdot 2^{64}$, and an enumeration of locally square values of $x^3 + y^7$ for small x and y.

1 Introduction

A rational number is **locally square** at a prime p if it is a square in the p-adic field $\mathbf{Q}_p$. In particular:

- A nonzero integer is locally square at 2 if and only if it is a square modulo $2, 4, 8, 16, \ldots$: equivalently, it has the form $2^{2e}s$ where s is an odd square modulo 8, i.e., $s \bmod 8 = 1$.
- A nonzero integer is locally square at an odd prime p if and only if it is a square modulo $p, p^2, p^3, p^4, \ldots$: equivalently, it has the form $p^{2e}s$ where s is a nonzero square modulo p, i.e., $s^{(p-1)/2} \bmod p = 1$.

A nonnegative rational number is a square if and only if it is locally square at every prime p.

Consider the problem of enumerating all integers x in a specified interval such that a specified polynomial in x is locally square at all primes below a specified bound. Consider, for example, the problem of enumerating all integers x between 0 and $10^{17} - 1$ such that $x^3 + 1$ is locally square at all primes in $\{2, 3, \ldots, 251\}$.

One can simply check, for each of the 10^{17} values of x, the local squareness of $x^3 + 1$. This is an example of what I call "unfocused enumeration."

2000 *Mathematics Subject Classification.* Primary 11Y16. Secondary 11Y70.

A standard improvement is to first compute the possibilities for x modulo some small integer m, then focus on the corresponding arithmetic progressions. For example, $x \bmod 5$ must be in $\{0, 2, 4\}$, so one can focus attention on the $10^{17}/5$ values of x with $x \bmod 5 = 0$, then the $10^{17}/5$ values of x with $x \bmod 5 = 2$, and finally the $10^{17}/5$ values of x with $x \bmod 5 = 4$, avoiding 40% of the work. Even better, there are only 18 possibilities for $x \bmod 55$, so one can focus attention on 18 arithmetic progressions modulo 55, avoiding more than 67% of the work. These are examples of what I call "focused enumeration."

The number of x's drops exponentially with the number of prime divisors of m: each additional prime reduces the number of x's by a factor of approximately 2. But the number of arithmetic progressions, and thus the overhead of considering each arithmetic progression, grows more than exponentially with the number of prime divisors. The minimum computation time is achieved for m somewhere around 10^{14}; the best choice of m depends on the relative costs of considering an arithmetic progression and considering an x.

The point of this paper is that another technique, which I call "doubly focused enumeration," makes the overhead much smaller, allowing m to be chosen much larger. For example, one can reasonably take $m \approx 3.1 \cdot 10^{25}$ as 8 times the product of all primes between 3 and 67, reducing the number of x's by a factor of about 66123.

Section 2 of this paper explains doubly focused enumeration in a more general setting. Section 3 returns to locally square polynomial values:

- It presents an algorithm that uses doubly focused enumeration to figure out which of $f(c+1), f(c+2), \ldots, f(c+H)$ are locally square at all primes $p \le h$, given a nonconstant squarefree polynomial f, an integer c, a positive integer H, and an integer $h \ge 2 \log H$.
- It proves that this algorithm typically takes time $H/M^{2+o(1)}$ where $M = H^{1/\lg \log H}$; here $\lg = \log_2$ as usual. More precisely: The average time for the algorithm, when c is a uniform random element of an interval of length about H^2, is $H/M^{2+o(1)}$ for fixed f as $H \to \infty$, provided that c has at most $M^{o(1)}$ digits and h is in $M^{o(1)}$. I do not know how to prove the same bound for a fixed c.

For comparison: Focused enumeration takes time $H/M^{1+o(1)}$.

Section 4 and Section 5 report, as examples of doubly focused enumeration, two record-setting computations. The first computation (December 2001) showed that every non-square positive integer below $24 \cdot 2^{64}$ is locally non-square at some prime in $\{2, 3, \ldots, 283\}$; this is numerical evidence for a standard conjecture related to fast deterministic primality proving. The second computation (February 2003 through April 2003) scanned $2 \cdot 10^{20}$ small pairs (x, y) to find locally square values of $x^3 + y^7$ with x, y coprime.

2 Doubly focused enumeration

Consider the general problem of finding all integers $x \in [1, H]$ such that $x \bmod m_1 \in S_1$ and $x \bmod m_2 \in S_2$. Here H is a positive integer; m_1 and m_2 are coprime positive integers; S_1 is a subset of $\mathbf{Z}/m_1$; and S_2 is a subset of $\mathbf{Z}/m_2$.

This section presents three solutions to this problem. The solutions do not have standard names; I call them "unfocused enumeration," "focused enumeration," and "doubly focused enumeration," as in Section 1.

In common applications, focused enumeration is asymptotically faster than unfocused enumeration, and doubly focused enumeration is asymptotically faster than focused enumeration.

The following sizes are typical for applications: $H \approx 10^{20}$; $m_1 \approx m_2 \approx 10^{14}$; and $\#S_1 \approx \#S_2 \approx 10^{11}$, so that $H(\#S_1/m_1)(\#S_2/m_2) \approx 10^{14}$. In many situations, one can prove that the number of outputs is approximately $H(\#S_1/m_1)(\#S_2/m_2)$; see, for example, Section 3.

Unfocused enumeration. The first method is to consider the possibilities $x = 1$, $x = 2$, $x = 3$, and so on, checking for each x in turn whether $x \bmod m_1 \in S_1$ and $x \bmod m_2 \in S_2$.

The sets S_1 and S_2 can be represented in the obvious way as circular arrays of m_1 and m_2 bits respectively. There is very little work for each new x: check the next bit in each array, and record x on the rare occasions that both bits are 1. Common general-purpose computers can check 32 or 64 values of x simultaneously.

Focused enumeration. The second method is to generate, for each $r \in S_1$, the arithmetic progression of $x \in [1, H]$ such that $x \bmod m_1 = r$, and then check for each x successively whether $x \bmod m_2 \in S_2$.

The advantage of focused enumeration over unfocused enumeration is that the number of operations drops from H to about $H(\#S_1/m_1) + m_1$. The disadvantage is that S_2 is no longer checked sequentially.

Doubly focused enumeration. The third method uses the following special case of the explicit Chinese remainder theorem: every integer $x \in [1, H]$ may be written as a difference between a reasonably small multiple of m_1 and a reasonably small multiple of m_2. More precisely: x may be written in the form $a_1 - a_2$, where a_1 is a multiple of m_1 in $[m_1, H + (m_1 - 1)m_2]$ and a_2 is a multiple of m_2 in $[0, (m_1 - 1)m_2]$. Notice that $x \bmod m_1 \in S_1$ if and only if $-a_2 \bmod m_1 \in S_1$, and $x \bmod m_2 \in S_2$ if and only if $a_1 \bmod m_2 \in S_2$.

Here is the algorithm. Enumerate, in increasing order, the multiples a_1 of m_1 in $[m_1, H + (m_1 - 1)m_2]$ such that $a_1 \bmod m_2 \in S_2$. Simultaneously enumerate, in increasing order, the multiples a_2 of m_2 in $[0, (m_1 - 1)m_2]$ such that $-a_2 \bmod m_1 \in S_1$. Merge these two lists to see all differences $a_1 - a_2$ in $[1, H]$.

The advantage of doubly focused enumeration over focused enumeration is that the number of operations drops from about $H(\#S_1/m_1) + m_1$ to, typically, about $H(\#S_1/m_1)(\#S_2/m_2) + m_1 + m_2$. The disadvantage is that each operation is fairly complicated: for example, a multidigit comparison.

This idea is so simple that it must have been written down before. However, I have not been able to locate it in the literature, and it is certainly not widely known in the context of enumerating locally square polynomial values.

Further factorization. In most applications, one can factor m_1 and m_2 into much smaller pieces, and correspondingly factor S_1 and S_2. Consider, for example, coprime positive integers m_{11} and m_{12} and sets S_{11} and S_{12} such that $m = m_{11}m_{12}$ and $S_1 = \{r : r \bmod m_{11} \in S_{11}, r \bmod m_{12} \in S_{12}\}$.

For unfocused enumeration: One can store S_{11} and S_{12} instead of S_1, using $m_{11} + m_{12}$ bits of memory instead of m_1 bits of memory. One then checks bits of S_1 by checking the corresponding bits of S_{11} and S_{12}.

For focused enumeration: One can enumerate values $r \in S_1$ more quickly than trying each $r \in \mathbf{Z}/m_1$, by applying the explicit Chinese remainder theorem to each pair in $S_{11} \times S_{12}$. This well-known technique again avoids the need to store S_1, and reduces the number of operations from about $H(\#S_1/m_1) + m_1$ to about $H(\#S_1/m_1) + \#S_1 + m_{11} + m_{12}$.

For doubly focused enumeration: The only extra difficulty is that values $r \in S_1$ need to be enumerated in increasing order. This can be done without much memory; see, e.g., [4].

3 Enumeration of locally square polynomial values

Fix a nonconstant squarefree polynomial f in one variable over $\mathbf{Z}$. Consider the problem of finding all integers $x \in [1, H]$ such that $f(c+x)$ is locally square at all primes $p \le h$, given a positive integer H, an integer c, and an integer $h \ge 2 \log H$.

Here is an algorithm for solving this problem. Select coprime positive integers m_1 and m_2 such that $p \le h$ for every prime p dividing $m_1 m_2$. Define S_1 as the set of $r \in \mathbf{Z}/m_1$ such that $f(c+r)$ is a square in $\mathbf{Z}/m_1$, and define S_2 as the set of $r \in \mathbf{Z}/m_2$ such that $f(c+r)$ is a square in $\mathbf{Z}/m_2$. Enumerate all integers $x \in [1, H]$ such that $x \bmod m_1 \in S_1$ and $x \bmod m_2 \in S_2$, as explained in Section 2. Check, for each such x, whether $f(c+x)$ is locally square at all primes $p \le h$.

The rest of this section shows that this algorithm takes time $H/M^{2+o(1)}$ for an average c under mild assumptions, if m_1 and m_2 are selected properly. Here $M = H^{1/\lg \log H}$, as in Section 1, and $o(1)$ is as $H \to \infty$ for f fixed.

Assume for simplicity that m_1 and m_2 are squarefree; that they are each in $H/M^{2+o(1)}$; that each prime p dividing $m_1 m_2$ is smaller than $2 \log H$; and that the number of p's is in $(2+o(1))(\log H)/\log\log H = (2+o(1)) \lg M$. Theorem 3.1 below explains one way to construct m_1 and m_2 satisfying these conditions.

Assume also that c has at most $M^{o(1)}$ digits and that h is in $M^{o(1)}$. The basic operations in the algorithm—checking whether $f(c+x)$ is a square modulo various primes, or is locally square at various primes—then take time $M^{o(1)}$ with negligible memory. (One can speed up the algorithm by using more memory, as discussed in Section 2, and by choosing m_1 and m_2 somewhat larger. However, the speedup is only $M^{o(1)}$, which is not visible at the level of precision of this analysis.)

There are three bottlenecks in the algorithm:

- Checking whether $f(c+x)$ is locally square at all primes $p \le h$, for each $x \in [1, H]$ such that $x \bmod m_1 \in S_1$ and $x \bmod m_2 \in S_2$, i.e., for each $x \in [1, H]$ such that $f(c+x)$ is a square modulo $m_1 m_2$. If c is a uniform random element of an interval of length $m_1 m_2$ then the average number of candidates x is at most $H/2^{(2+o(1)) \lg M} = H/M^{2+o(1)}$ by Theorem 3.3 below.
- Checking whether $a_1 \bmod m_2$ is in S_2, for each multiple a_1 of m_1 between m_1 and $H + (m_1 - 1)m_2$. There are $H/M^{2+o(1)}$ multiples to check.
- Checking whether $-a_2 \bmod m_1$ is in S_1, for each multiple a_2 of m_2 between 0 and $(m_1 - 1)m_2$. There are $H/M^{2+o(1)}$ multiples to check.

The total time is $H/M^{2+o(1)}$ if c is a uniform random element of an interval of length $m_1 m_2 \approx H^2$.

Theorem 3.1 *Let H be a positive integer. Define $u = \log H$; assume that $2u \ge 41$. Define $M = \exp(u/\lg u)$. Let v be the largest integer such that the product m of the primes in $[1, v]$ satisfies $m \le H^2/M^4$. Let v_1 be the largest integer such that the product m_1 of the primes in $[1, v_1]$ satisfies $m_1 \le H/M^2$. Then there are*

$(2+o(1))u/\log u$ prime divisors of m; all prime divisors of m are smaller than $2u$; and both m_1 and m/m_1 are in $H/M^{2+o(1)}$.

One can quickly compute four possibilities for $(v, v_1, m_1, m/m_1)$ by computing approximations to u and M.

Proof The prime number theorem implies that v is in $(1+o(1))\log(H^2/M^4) = (2+o(1))u$. Thus there are $(2+o(1))u/\log 2u = (2+o(1))u/\log u$ prime divisors of m. Furthermore, $m(v+1) > H^2/M^4$ by definition of v, so m is in $H^2/M^{4+o(1)}$; by the same argument, m_1 is in $H/M^{2+o(1)}$; so m/m_1 is also in $H/M^{2+o(1)}$.

Apply one of the Rosser-Schoenfeld theorems (see [16, Theorem 4]): the product of the primes in $[1, 2u]$ is larger than $\exp(2u(1 - 1/\log 2u))$ since $2u \geq 41$. But $\log 2u > \log u > (1/2)\lg u$, so $\exp(2u/\log 2u) < \exp(4u/\lg u) = M^4$; hence the product of the primes in $[1, 2u]$ is larger than H^2/M^4. Consequently $v < 2u$. $\square$

Theorem 3.2 *Let d be a positive integer. Let f be a polynomial of degree d over $\mathbf{Z}$. Let p be an odd prime number that does not divide the leading coefficient of f and does not divide the discriminant of f. Then there are at most $(p+(d-1)\sqrt{p}+d)/2$ elements r of $\mathbf{Z}/p$ such that $f(r)$ is a square in $\mathbf{Z}/p$.*

Proof Define $\chi : \mathbf{Z}/p \to \{-1, 0, 1\}$ as the Legendre symbol modulo p; X_i as $\{r \in \mathbf{Z}/p : \chi(f(r)) = i\}$; a as the leading coefficient of f; and g as the polynomial $a^{-1}f$ over the field $\mathbf{Z}/p$.

Check the conditions of Weil's theorem, as stated in [12, Theorem 5.41]: χ is a multiplicative character of $\mathbf{Z}/p$ of order 2; g is a monic polynomial over $\mathbf{Z}/p$ of positive degree (namely, degree d); g is not a square, because otherwise p would divide the discriminant of f; and g has at most d (in fact, exactly d) distinct roots in its splitting field over $\mathbf{Z}/p$.

Conclusion: $X_1 - X_{-1} = \sum_r \chi(f(r)) = \sum_r \chi(ag(r))$ is at most $(d-1)\sqrt{p}$. But $X_1 + X_0 + X_{-1}$ is exactly p; and X_0 is exactly the number of roots of f in $\mathbf{Z}/p$, which is at most d. Add: $2X_1 + 2X_0 \leq p + (d-1)\sqrt{p} + d$. $\square$

Theorem 3.3 *Let f be a nonconstant squarefree polynomial over $\mathbf{Z}$. Then there is a function $\epsilon : \mathbf{N} \to \mathbf{R}$, with $\epsilon \in o(1)$, such that $f(r)$ is a square in $\mathbf{Z}/m$ with probability at most $2^{-(1+\epsilon(k))k}$ if m is a squarefree positive integer, k is the number of prime divisors of m, and r is a uniform random element of $\mathbf{Z}/m$.*

Proof Write $d = \deg f \geq 1$. Note that the discriminant of f is nonzero. Define α as the maximum of the following quantities: d; $\sqrt{2}$; $\sqrt{p}$ for the primes p dividing the discriminant of f; and $\sqrt{p}$ for the primes p dividing the leading coefficient of f.

I claim that if p is prime and $r \bmod p$ is uniform then $f(r)$ is a square modulo p with probability at most $(1+\alpha/\sqrt{p})/2$. Indeed, if $p > d^2$ is an odd prime that divides neither the discriminant of f nor the leading coefficient of f, then the probability is at most

$$\frac{1}{2}\left(1 + \frac{d-1}{\sqrt{p}} + \frac{d}{p}\right) < \frac{1}{2}\left(1 + \frac{d}{\sqrt{p}}\right) \leq \frac{1}{2}\left(1 + \frac{\alpha}{\sqrt{p}}\right)$$

by Theorem 3.2. Otherwise $\sqrt{p} \leq \alpha$ by definition of α; the probability is at most $1 \leq (1+\alpha/\sqrt{p})/2$.

The probability that $f(r)$ is a square modulo m is the product, over the primes p dividing m, of the probability that $f(r)$ is a square modulo p; which is at most the product of $(1+\alpha/\sqrt{p})/2$ for these k primes p; which is, in turn, at most

$(1+\alpha/\sqrt{2})(1+\alpha/\sqrt{3})(1+\alpha/\sqrt{4})\cdots(1+\alpha/\sqrt{k+1})/2^k$; in other words, at most $2^{-(1+\epsilon(k))k}$, where $\epsilon(0)=0$ and

$$\epsilon(k) = \frac{-1}{k}\left(\lg\left(1+\frac{\alpha}{\sqrt{2}}\right)+\lg\left(1+\frac{\alpha}{\sqrt{3}}\right)+\cdots+\lg\left(1+\frac{\alpha}{\sqrt{k+1}}\right)\right)$$

for $k \ge 1$. The sum $\log(1+\alpha/\sqrt{2})+\cdots+\log(1+\alpha/\sqrt{k+1}) \le \alpha/\sqrt{2}+\cdots+\alpha/\sqrt{k+1}$ is bounded by a multiple of $\sqrt{k+1}$, so $\epsilon(k)\to 0$ as $k\to\infty$. □

4 Example: locally square integers

Let x be a positive non-square integer in $1+8\mathbf{Z}$. What is the smallest odd prime r such that $x^{(r-1)/2} \bmod r \ne 1$? In other words, what is the smallest odd prime r such that x is divisible by r or locally non-square at r or both?

It is widely conjectured that $r/\log r$ is at most $(1+o(1))\lg x$, where $\lg = \log_2$. In fact, no examples are known in which $r/\log r$ is larger than $\lg x$. A proof of an explicit bound such as $r/\log r \le 2\lg x$ would imply, among other things, that there is a deterministic primality-proving algorithm taking essentially cubic time. See [8], [2], [14, pages 130–136], and [15, Section 2].

I have verified that $r \le 283$ for all $x < 24\cdot 2^{64} \approx 4.4\cdot 10^{20}$. Here are the cutoffs for each r between 181 and 281 inclusive:

$r \le$	$r/\log r <$	if $x <$
181	34.818	$696161110209049 \approx 1.237\cdot 2^{49}$
193	36.674	$2854909648103881 \approx 1.268\cdot 2^{51}$
197	37.288	$6450045516630769 \approx 1.432\cdot 2^{52}$
211	39.426	$11641399247947921 \approx 1.292\cdot 2^{53}$
227	41.844	$190621428905186449 \approx 1.323\cdot 2^{57}$
229	42.145	$196640248121928601 \approx 1.364\cdot 2^{57}$
233	42.745	$712624335095093521 \approx 1.236\cdot 2^{59}$
239	43.642	$1773855791877850321 \approx 1.539\cdot 2^{60}$
241	43.940	$2327687064124474441 \approx 1.009\cdot 2^{61}$
251	45.427	$6384991873059836689 \approx 1.385\cdot 2^{62}$
257	46.315	$8019204661305419761 \approx 1.739\cdot 2^{62}$
263	47.199	$10198100582046287689 \approx 1.106\cdot 2^{63}$
277	49.254	$69848288320900186969 \approx 1.893\cdot 2^{65}$
281	49.838	$208936365799044975961 \approx 1.416\cdot 2^{67}$
283	50.129	$24\cdot 2^{64} = 1.5\cdot 2^{68}$(not maximal)

This computation took ten days, about $1.2\cdot 10^{15}$ clock cycles, on a Pentium 4 running at 1406MHz.

Another way to phrase the same result: Every non-square positive integer below $24\cdot 2^{64}$ is locally non-square at some prime in $\{2,3,\ldots,283\}$. Indeed, write the integer in the form xy^2 where x is squarefree. If x is a square then the original integer is a square, contradiction. If $x \notin 1+8\mathbf{Z}$ then xy^2 is locally non-square at 2. If x is a non-square in $1+8\mathbf{Z}$ then, by this computation, there is an odd prime $r \le 283$ for which $x^{(r-1)/2} \bmod r \ne 1$. If $x^{(r-1)/2} \bmod r = r-1$ then x is locally non-square at r. If $x^{(r-1)/2} \bmod r = 0$ then x is divisible by r but, being squarefree, not by r^2, so it is locally non-square at r.

A series of previous computations, initiated by Kraitchik in 1924 and continued by Lehmer, Lehmer, Shanks, Patterson, Williams, Stephens, and Lukes, showed with considerably more effort that $r \le 281$ for all x up to about $7\cdot 10^{19} \approx 2^{66}$. See

[9], [10], [11], [17], [14, page 134], and [15]. For example, the computation of Lukes, Patterson, and Williams in [15] was a focused enumeration of all small y such that $1+24y$ is a non-unit square modulo $m_1 = 5\cdot 7\cdot 11\cdot 13$; there are about $H/27$ such values of y in $[1,H]$.

My computation was a doubly focused enumeration, as explained in Section 2 and Section 3, of all small y such that $1+24y$ is a non-unit square modulo both $m_1 = 41\cdot 43\cdot 47\cdot 53\cdot 59\cdot 61\cdot 71\cdot 73$ and $m_2 = 5\cdot 7\cdot 11\cdot 13\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 37\cdot 67$. There are about $H/1386487$ such values of y in $[1,H]$.

Further speed improvements are possible. I could use somewhat larger moduli m_1 and m_2, for example, especially if I balance the primes.

A note on terminology: pseudosquares. Lehmer in [10] defined, for each prime $q \ge 3$, the corresponding "pseudo-square" L_q as the smallest positive non-square integer $x \in 1+8\mathbf{Z}$ for which $r > q$, i.e., for which $x^{(p-1)/2} \bmod p = 1$ for all primes $p \le q$. The same terminology is used in [18, page 522], [14], and [15].

On the other hand, Lehmer, Lehmer, and Shanks in [11] defined a "pseudo-square" for q as *any* non-square integer $x \in 1+8\mathbf{Z}$ for which $r > q$. The same terminology is used in [5]. The "Table of Pseudo-Squares" in [11, page 434] includes one "least solution" column and one "least prime solution" column. A "prime pseudo-square" in this terminology does not have a short name in the previous terminology.

"Pseudo-squares" have an unrelated definition in [1] and [3]: a sequence of "pseudo-squares" is a sequence of integers in which the nth integer is close to n^2 in the usual metric.

5 Example: locally square values of $x^3 + y^7$

The problem here is to find all small coprime integer pairs (x, y) such that $x^3 + y^7$ is locally square at all primes $p < 300$. This is inspired by the well-known problem, discussed in [6], of finding all coprime integer pairs (x, y) for which x^3+y^7 is a square.

I searched $2\cdot 10^{20}+2$ pairs (x, y): the range $x \in [-y^3, 10^{17}-1-y^3]$ for each $y \in [1, 1000]$, the range $x \in [0, 10^{17}-1]$ for each $y \in [-1000, -1]$, and the range $x \in \{-1, 1\}$ for $y = 0$. Results:

$$
\begin{array}{rrll}
15163605661652121^3 + & (-980)^7 = & \text{non-square} & \text{(new)} \\
33408736951858326^3 + & (-503)^7 = & \text{non-square} & \text{(new)} \\
81737917855133193^3 + & (-236)^7 = & \text{non-square} & \text{(new)} \\
14380086519066498^3 + & (-47)^7 = & \text{non-square} & \text{(new)} \\
1^3 + & (-1)^7 = & 0^2 & \\
1^3 + & 0^7 = & 1^2 & \\
(-1)^3 + & 1^7 = & 0^2 & \\
0^3 + & 1^7 = & 1^2 & \\
2^3 + & 1^7 = & 3^2 & \\
17^3 + & 2^7 = & 71^2 & \\
76271^3 + & 17^7 = & 21063928^2 & \text{(Beukers and Zagier, 1993)} \\
(-1414)^3 + & 65^7 = & 2213459^2 & \text{(Beukers and Zagier, 1993)} \\
(-9262)^3 + & 113^7 = & 15312283^2 & \text{(Beukers and Zagier, 1993)} \\
38113906696577086^3 + & 225^7 = & \text{non-square} & \text{(new)} \\
45622146410700257^3 + & 892^7 = & \text{non-square} & \text{(new)} \\
2129085874168881^3 + & 940^7 = & \text{non-square} & \text{(new)}
\end{array}
$$

Computational details: Define $m = 3 \cdot 5 \cdot 7 \cdot 8 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 47 \cdot 53 \cdot 59 \cdot 61 \cdot 67 \approx 3.1433 \cdot 10^{25}$. For each y separately, I did a doubly focused enumeration of x coprime to $\gcd\{y, m\}$ such that $x^3 + y^7$ is a square modulo m. This enumeration produced only a small fraction of the original 10^{20} pairs (x, y). I then checked, for each enumerated x, whether $x^3 + y^7$ is locally square at all primes $p < 300$, and whether x is coprime to y.

References

[1] A. O. L. Atkin, *On pseudo-squares*, Proceedings of the London Mathematical Society, Third Series **14a** (1965), 22–27. ISSN 0024–6115. MR 34:2547.

[2] Eric Bach, Lorenz Huelsbergen, *Statistical evidence for small generating sets*, Mathematics of Computation **61** (1993), 69–82. ISSN 0025–5718. MR 93k:11089. Available from `http://www.jstor.org/sici?sici=0025-5718(199307)61:203<69:SEFSGS>2.0.CO;2-3`.

[3] R. Balasubramanian, D. S. Ramana, *Atkin's theorem on pseudo-squares*, Institut Mathématique, Publications, Nouvelle Série **63** (1998), 21–25. ISSN 0350–1302. MR 99e:11012.

[4] Daniel J. Bernstein, *Enumerating solutions to* $p(a) + q(b) = r(c) + s(d)$, Mathematics of Computation **70** (2001), 389–394. ISSN 0025–5718. Available from `http://cr.yp.to/papers.html`.

[5] Nathan D. Bronson, Duncan A. Buell, *Congruential sieves on FPGA computers*, in [7] (1994), 547–551. MR 95k:11165.

[6] Henri Darmon, Andrew Granville, *On the equations* $z^m = F(x, y)$ *and* $Ax^p + By^q = Cz^r$, Bulletin of the London Mathematical Society **27** (1995), 513–543. ISSN 0024–6093. MR 96e:11042. Available from `http://www.math.mcgill.ca/~darmon/pub/pub.html`.

[7] Walter Gautschi (editor), *Mathematics of Computation 1943–1993: a half-century of computational mathematics*, American Mathematical Society, Providence, 1994. ISBN 0–8218–0291–7. MR 95j:00014.

[8] Marshall Hall, *Quadratic residues in factorization*, Bulletin of the American Mathematical Society **39** (1933), 758–763. ISSN 0273–0979. Available from `http://cr.yp.to/bib/entries.html#1933/hall`.

[9] Derrick H. Lehmer, *The mechanical combination of linear forms*, American Mathematical Monthly **35** (1928), 114–121. ISSN 0002–9890. Available from `http://links.jstor.org/sici?sici=0002-9890(192803)35:3<114:TMCOLF>2.0.CO;2-Z`.

[10] Derrick H. Lehmer, *A sieve problem on "pseudo-squares"*, Mathematical Tables and Other Aids to Computation **8** (1954), 241–242. ISSN 0891–6837. MR 16,113e. Available from `http://links.jstor.org/sici?sici=0891-6837(195410)8:48<237:N>2.0.CO;2-R`.

[11] Derrick H. Lehmer, Emma Lehmer, Daniel Shanks, *Integer sequence having prescribed quadratic character*, Mathematics of Computation **24** (1970), 433–451. ISSN 0025–5718. MR 42:5889. Available from `http://links.jstor.org/sici?sici=0025-5718(197004)24:110<433:ISHPQC>2.0.CO;2-G`.

[12] Rudolf Lidl, Harald Niederreiter, *Finite fields*, 2nd edition, Encyclopedia of Mathematics and its Applications, 20, Cambridge University Press, Cambridge, 1997. ISBN 0–521–39231–4. MR 97i:11115.

[13] John H. Loxton (editor), *Number theory and cryptography*, London Mathematical Society Lecture Note Series, 154, Cambridge University Press, Cambridge, 1990. ISBN 0–521–39877–0. MR 90m:11003.

[14] Richard F. Lukes, C. D. Patterson, Hugh C. Williams, *Numerical sieving devices: their history and some applications*, Nieuw Archief voor Wiskunde Series 4 **13** (1995), 113–139. ISSN 0028–9825. MR 96m:11082. Available from `http://cr.yp.to/bib/entries.html#1995/lukes`.

[15] Richard F. Lukes, C. D. Patterson, Hugh C. Williams, *Some results on pseudosquares*, Mathematics of Computation **65** (1996), 361–372. ISSN 0025–5718. MR 96e:11010. Available from `http://www.ams.org/jourcgi/jour-getitem?pii=S0025571896006783`.

[16] J. Barkley Rosser, Lowell Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois Journal of Mathematics **6** (1962), 64–94. ISSN 0019–2082. MR 25:1139. Available from `http://cr.yp.to/bib/entries.html#1962/rosser`.

[17] A. J. Stephens, Hugh C. Williams, *An open architecture number sieve*, in [13] (1990), 38–75.

[18] Hugh C. Williams, Jeffrey O. Shallit, *Factoring integers before computers*, in [7] (1994), 481–531. MR 95m:11143.