AI-assisted third draft for author review

Two 37-digit strong pseudoprimes to the first twenty prime bases

Tyler Hughes *Coauthorship to be confirmed*

Abstract

The first twelve prime bases suffice to test every unsigned 64-bit integer for primality. The first twenty fail well within 128 bits. We give two 37-digit counterexamples, each the product of primes p and $2p-1$. Both pass every prime base through 71. Base 73 separates the powers of two in the two multiplicative orders and detects both composites, even though both still pass its Fermat test. The smaller product gives $\psi_{20} < 2^{121}$, where ψ_{20} denotes the least odd composite passing all twenty bases. The proof consists of short primality certificates and modular powers checked in Lean 4. Finding the products required a much larger computation. A residue sieve extended Zhang's search in this family from 10^{36} to 10^{37} and returned exactly these two products. A second implementation repeated 64 of its 1,024 parts. A finite-field character sum explains how the next prime base changes the residue classes available to the sieve. It also gives a model for the variation in Zhang's counts.

MSC 2020 11Y11, 11A51, 11Y16 **Keywords** strong pseudoprimes, primality testing, character sums.

1 Two factorizations

When a composite passes a primality test, the smallest such composite marks the end of the range on which the test is decisive. We set aside the elementary cases of integers below two and prime divisors of the chosen bases, which can be checked directly. Sorenson and Webster determined this threshold for the first twelve prime bases. It exceeds 2^{64} [5]. Can eight more bases cover a word twice as wide? Two factorizations answer the question.

Theorem 1. *For each of the following primes p, the integer $q = 2p-1$ is prime and the product $n = pq$ passes the strong probable-prime test to each of the first twenty prime bases. Both products fail at the next prime,* 73*.*

p	$n = p(2p-1)$	*size*
1113813905784150541	2481162833436289154832260656117034821	121 *bits*
1726253494836549181	5959902256870799858089729225626992341	123 *bits*

Thus the smaller product, n_1, is an upper bound for ψ_{20}.

For either witness $n-1 = 4d$ with d odd. The strong test therefore accepts if any of three congruences holds, $b^d = 1$, $b^d = -1$, or $b^{2d} = -1$, all modulo n. The following code verifies the two factorizations as compositeness witnesses and tests both products at all twenty-one bases. The order criterion in Section 2 explains its outcome.

```
bases = (2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71)
for p in (1113813905784150541, 1726253494836549181):
    n = p * (2*p - 1)
    d, rem = divmod(n - 1, 4)
    assert rem == 0 and d % 2 == 1 and 1 < p < n < 2**127
    def passes(b):
        x = pow(b, d, n)
        return x in (1, n-1) or x*x % n == n-1
    assert all(passes(b) for b in bases) and not passes(73)
```

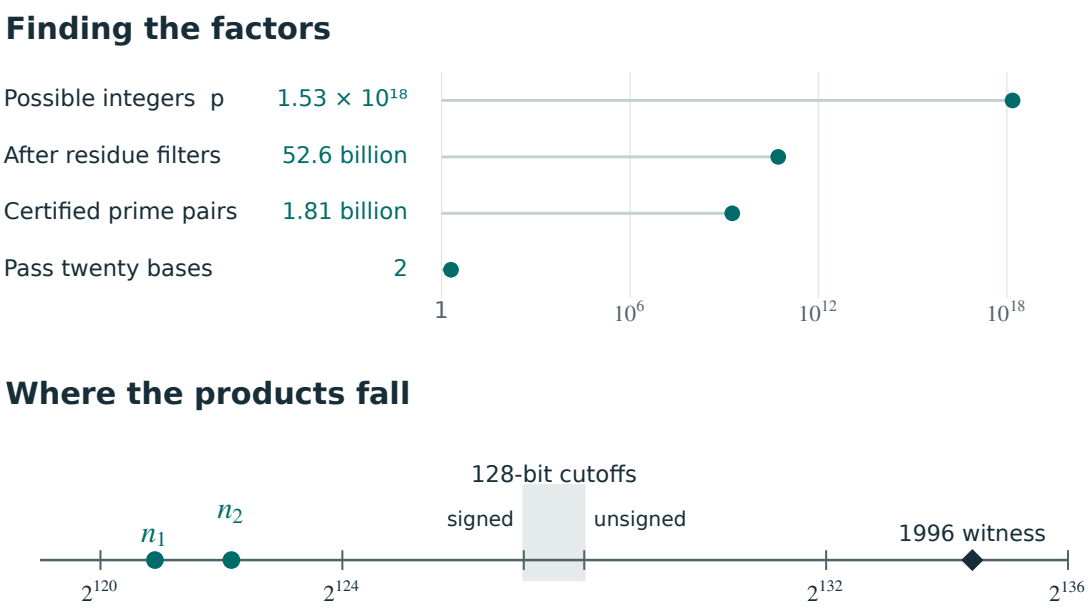


Figure 1. The search and its two witnesses. Above, the horizontal scale counts candidates. Residue filters apply to the smaller factor p, the primality tests to p and $2p-1$, and the last twenty tests to their product. Below, each doubling occupies the same distance. The two products lie below both 128-bit cutoffs. Bleichenbacher's earlier witness lies above them. Each new point has a direct arithmetic certificate. Only the count of points in the search interval depends on the full enumeration.

2 Why the orders must agree

Write $n-1=2^s d$, d odd, and suppose $\gcd(b,n)=1$. The strong test for an odd $n>2$ accepts if $b^d=1 \bmod n$ or if $b^{2^i d}=-1 \bmod n$ for some $0\le i<s$. For a prime factor r, let $t_r=v_2(\operatorname{ord}_r b)$, the exponent of two in the multiplicative order of b mod r. After the odd part of the order has been removed, t_r counts how many squarings it takes to reach 1. Two prime factors must give the same answer at the same step. Jaeschke proved this signature criterion for squarefree integers and gave the Fermat criterion below for this family, including the restriction at base two [3, Propositions 1 and 4].

Lemma 2. *Let p and $q=2p-1$ be odd primes, $n=pq$, and $\gcd(b,n)=1$. The Fermat test $b^{n-1}=1 \bmod n$ accepts exactly when b is a square modulo q. The strong test accepts exactly when $t_p=t_q$.*

Proof. Put $p-1=2^e u$, u odd. Then $q-1=2^{e+1}u$ and $n-1=(2p+1)(p-1)$. Modulo p, Fermat's congruence holds for every unit. Modulo q, Euler's criterion gives $b^{p-1}=\left(\frac{b}{q}\right)$, and raising to the odd power $2p+1$ preserves this sign. For the strong test the odd exponent is $d=(2p+1)u$. It removes the odd part of each order. If both resulting orders are 1, the first test passes. If both are $2^t>1$, exactly $t-1$ squarings give -1 at both primes. Here $t\le e$, so the test reaches that step. If the orders differ, one component reaches 1 while the other still has even order, and the components cannot reach -1 together. The Chinese remainder theorem gives the result. □

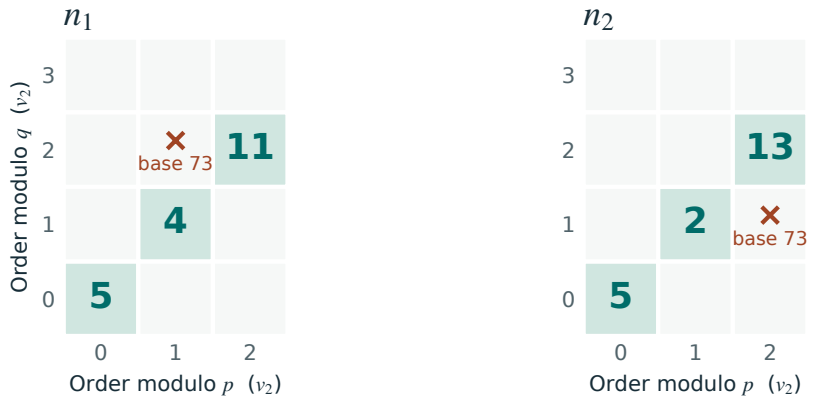


Figure 2. Each base through 71 contributes one observation to a diagonal cell. The number in a cell counts bases. The cross locates 73. At n_1 the order modulo q needs one more squaring than the order modulo p. At n_2 it needs one fewer. In each case base 73 is still a square modulo q, so Fermat's test accepts.

Counting bases. For $r-1 = 2^E u$ with u odd, a uniformly chosen unit has $t_r = 0$ with probability 2^{-E}. For $1 \le k \le E$ it has $t_r = k$ with probability 2^{k-1-E}. These are counts in a cyclic group. The two coordinates of a uniform unit modulo pq are independent. Multiplying the matching probabilities gives the exact fraction that pass the strong test,

$$2^{-2e-1}\left(1+\sum_{k=1}^{e} 4^{k-1}\right) = \frac{1+2\,4^{-e}}{6}.$$

At $e=1$ the share is $1/4$, but $p = 3 \bmod 4$ then forces $q = 5 \bmod 8$, so base two fails even the Fermat test. Every pair of interest has $p = 1 \bmod 4$. The largest surviving share is $3/16$, at $e=2$, the value for both of our witnesses. Both fractions also appear in Zhang's analysis [6].

3 Certificates for the two products

The two displayed products are visibly composite. To put them in the search family $K_2 = \{p(2p-1) : p, 2p-1 \text{ prime},\ p > 2\}$, we must also certify their factors. A Pratt certificate gives a short proof of this fact [4]. At a node r factor $r-1$ completely and find a unit a with

$$a^{r-1} = 1 \bmod r, \qquad a^{(r-1)/\ell} \neq 1 \bmod r \quad \text{for every prime } \ell \mid r-1.$$

The order of a must be $r-1$, which forces $\varphi(r) = r-1$. One applies the same criterion to the factors ℓ until they are small enough for trial division. Since $q-1 = 2(p-1)$, both factors of each product share the odd part of their certificate.

Node	Witness a	Factorization of node minus one
p_1	2	$2^2 \cdot 3 \cdot 5 \cdot r_1$
q_1	101	$2^3 \cdot 3 \cdot 5 \cdot r_1$
p_2	10	$2^2 \cdot 3 \cdot 5 \cdot 181 \cdot r_2$
q_2	89	$2^3 \cdot 3 \cdot 5 \cdot 181 \cdot r_2$

Here $r_1 = 18563565096402509$ and $r_2 = 158955202102813$. The full recursive certificates are supplied with the computation. They contain twelve non-leaf nodes in total. Checking the certificates, multiplying the factors, and evaluating the displayed strong test proves Theorem 1. Figure 2 gives an independent way to do the last step.

4 Finding the witnesses

Zhang completed the K_2 search through 10^{36} [6]. We searched the next decimal interval $10^{36} < p(2p-1) \le 10^{37}$. Lemma 2 supplies a cheap necessary condition for each odd prime base $b \le 71$. Since $q = 1 \bmod 4$, quadratic reciprocity gives $\left(\frac{b}{q}\right) = \left(\frac{2p-1}{b}\right)$. We can discard a residue class of $p \bmod b$ as soon as this symbol differs from $+1$. We also discard $p = 0 \bmod b$, because the entire search interval has $p > b$.

A count before any primality test. The map $x \mapsto 2x - 1$ permutes $\mathbb{F}_b$. Requiring a nonzero square leaves $(b-1)/2$ choices. Excluding $x = 0$ removes one more choice precisely when -1 is a square. Thus the number of allowed classes is

$$A(b) = \frac{b - 2 - \left(\frac{-1}{b}\right)}{2}.$$

The first wheel combines $p = 1 \bmod 4$ with the conditions at primes from 3 through 31. The Chinese remainder theorem gives 10,135,125 allowed classes modulo 401,120,980,260. A second wheel handles $37, 41, 43$, and direct lookups handle the remaining primes through 71. Each surviving p is tested along with $2p-1$. Both are below 2^{62}, within the proven range of the twelve-base test [5]. Applying the strong test to the surviving products gives the counts in Figure 1.

How much was checked twice. The primary program completed all 1,024 parts. Another implementation used a different wheel and a different deterministic primality test for the factors. It reproduced every common count and both hit lines in 62 parts selected from the primary summaries before the verification run, including boundary and extreme counts, plus the two parts containing the hits. Both programs use GMP for large modular powers. A separate control changed the sieve to require a square modulo p in place of q. The correct program recovered all 24 of Zhang's benchmark rows in windows about the known factors. The altered program recovered none.

Write ψ'_t for the least K_2 number passing the first t prime bases. Subject to the correctness of Zhang's search and the new enumeration, $\psi'_{20} = n_1$ and $\psi'_{21} > 10^{37}$. For unrestricted odd composites, the proven conclusion is $\psi_{20} \le n_1$. There are more families to rule out before that inequality can be replaced by an equality.

5 Why different bases discard different fractions

At an odd prime base b, two questions constrain a pair of factors: is $x = p \bmod b$ a square, and is $2x - 1$ a square? Only the latter is required by the wheel. The answers are correlated. This correlation enters the predicted survival rate because the two possible answers to the first question leave different chances of matching the orders.

Let χ be the quadratic character of $\mathbb{F}_b$, with $\chi(0) = 0$. Write N_{-+} and N_{++} for the numbers of x with the indicated signs of $\chi(x), \chi(2x-1)$. Then

$$N_{-+} + N_{++} = A(b), \qquad N_{-+} - N_{++} = \chi(2).$$

Indeed $8x(2x-1) = (4x-1)^2 - 1$. The conic $v^2 = u^2 - 1$ has $b-1$ points, one for each nonzero $u+v$, since $(u+v)(u-v) = 1$. Counting first over u gives $\sum_u \chi(u^2-1) = -1$, so $\sum_x \chi(x)\chi(2x-1) = -\chi(2)$. Also $\sum_{x \neq 0,1/2} \chi(x) = -\chi(2)$. Their half-sum is $N_{++} - N_{-+}$, as claimed. At $b = 3, 5$, for instance, only the $++$ cell survives.

From residue counts to a model. Both new pairs have $v_2(p-1) = 2$. Within this class the model treats admissible residues of prime pairs as uniform, and higher power-residue choices as independent subject to the two signs. For a nonsquare at p, the order there has binary exponent two. Among squares modulo q half have that exponent. For a square at p, exponents zero and one are equally likely. Modulo q, a square has each of those exponents with probability $1/4$. Thus this class has modeled pass fraction

$$S_2(b) = \frac{N_{-+}/2 + N_{++}/4}{b-2}.$$

The denominator counts the residues left after excluding $p = 0$ and $2p-1 = 0 \bmod b$. The fraction is $1/4$ at 3 and $1/12$ at 5. The sign $\chi(2)$ introduces variation with $b \bmod 8$. The character sums above are exact. Equidistribution along prime pairs and independence across successive bases are assumptions of the model.

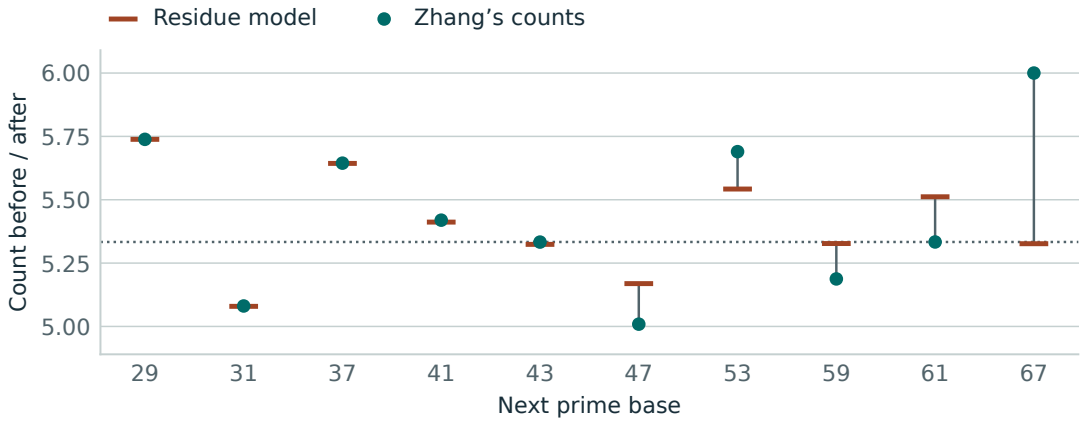


Figure 3. All points use Zhang's single cutoff 10^{36}. A count before a base divided by the count after it measures attrition. Dots are observed ratios, short strokes are the predictions from all modeled classes, and the dotted line is the constant $16/3$. The last ratio is $24/4$. Changes of a single survivor have a visible effect there.

For completeness, in class $e \geq 2$ put $h_e = (1+8\,4^{-e})/6$. The same count within the subgroup of squares gives $S_e(b) = (N_{-+}/2 + h_e N_{++})/(b-2)$. At base two the quadratic supplement changes the starting weight. The model uses $S_2(2) = 1/2$ and $S_e(2) = h_e$ for $e \geq 3$. With b_i the i-th prime, $\sum_{e \geq 2} 2^{-e} \prod_{i \leq t} S_e(b_i)$ is the predicted fraction of prime pairs surviving t bases. Figure 3 plots ratios of successive values. Multiplying this fraction by the Bateman–Horn estimate for prime pairs gives an expected 1.614 twenty-base survivors in the new interval. The search found two. The search itself never uses these probabilities to reject a candidate.

6 What a restricted search can settle

Zhang conjectured $\psi_t = \psi_t'$ for $t \geq 12$ [6]. One can test this against other pairs with $p = Bm+1$, $q = Am+1$ for coprime $A > B > 0$. If a base c passes the strong test for pq, its orders at

p and q have equal binary exponents. When $v_2(A) > v_2(B)$ this forces c to be a square at q, and when $v_2(A) < v_2(B)$ it forces a square at p. Equal valuations require matching Legendre signs: a unit is a nonsquare at a prime precisely when its order contains the full power of two dividing the group size. These necessary conditions make a residue sieve possible for each ratio.

A separate, single-implementation search tested $A/B \in \{3, 4, 5, 6, 3/2, 4/3, 5/2\}$, with $p > 173$ and $pq \le \psi'_{17}$. For $14 \le t \le 17$ it found no pair below the corresponding ψ'_t that passed t bases. Other ratios and composites with more prime factors remain possible. At twenty-one bases a single witness inside a 128-bit word would settle insufficiency. Exhausting one family without a witness leaves sufficiency open.

The historical comparison. Zhang's published limit is a lower bound in a specified family. Bleichenbacher's earlier upper bound for the unrestricted problem is a different comparison. Table 3.2 of his dissertation lists a 41-digit composite passing the first twenty-one prime bases [2]. Its ratio to n_1 is about 11,727. Arnault's journal construction passes many more bases and gives a larger number [1]. The shorter thesis witness is the relevant numerical benchmark. The literature check leaves gaps in Chinese-language journal coverage, so we make no exhaustive priority claim.

7 Formal verification and reproducibility

The Lean 4 library `lean/SpspPsi20` proves the primality of the four factors, the strong tests for the first twenty-one prime bases, the upper bound for ψ_{20}, the order criterion, the unit-group counts and the finite-field identities. The audit at commit `29f4789e` covers all 90 public declarations, with the three standard logical axioms and no unproved placeholders or native-code decisions. The enumeration and the distribution model are external to these theorems.

From this draft's directory, `python3 recompute.py` executes the printed example and checks both Pratt certificates. The program `figures/make_figures.py` redraws the three figures. The accompanying ledgers identify the search records and the literature consulted. AI systems assisted with the calculations, formalization, figures and drafting. The manuscript awaits review by its authors.

References

[1] F. Arnault, *Rabin–Miller primality test: Composite numbers which pass it*, Math. Comp. **64** (1995), no. 209, 355–361, DOI: 10.1090/S0025-5718-1995-1260124-2, Zbl 0813.11071, MR1260124.

[2] D. Bleichenbacher, *Efficiency and security of cryptosystems based on number theory*, Ph.D. thesis, Diss. ETH No. 11404, Swiss Federal Institute of Technology (ETH) Zürich, 1996, `https://cr.yp.to/bib/1996/bleichenbacher-thesis.pdf`.

[3] G. Jaeschke, *On strong pseudoprimes to several bases*, Math. Comp. **61** (1993), no. 204, 915–926, DOI: 10.1090/S0025-5718-1993-1192971-8, Zbl 0802.11001, MR1192971.

[4] V. R. Pratt, *Every prime has a succinct certificate*, SIAM J. Comput. **4** (1975), no. 3, 214–220, DOI: 10.1137/0204018, Zbl 0316.68031, MR0389738.

[5] J. P. Sorenson and J. Webster, *Strong pseudoprimes to twelve prime bases*, Math. Comp. **86** (2017), no. 304, 985–1003, DOI: 10.1090/mcom/3134, Zbl 1370.11140, MR3584557.

[6] Z. Zhang, *Two kinds of strong pseudoprimes up to* 10^{36}, Math. Comp. **76** (2007), no. 260, 2095–2107, DOI: 10.1090/S0025-5718-07-01977-1, Zbl 1131.11082, MR2336285.