Solutions to Daily Due Sep 23 (AI generated)

Math 4440/5440, Coding and Cryptography, Fall 2026

Generated by Claude for Katherine E. Stange
(all computations computer-verified)

Problems 2, 3 and 4 are about poster and project logistics. Problem 7, the Chaitin/Kolmogorov proof that there are infinitely many primes, is written up in the textbook (Section 3.7), so it is not repeated here.

Problem 1: finding $x^2 \equiv y^2 \pmod{n}$ with $x \not\equiv \pm y$, and which n allow it

Examples

Hunting with the playground or Sage turns up, for instance,

n	x	y	a factor: $\gcd(x-y, n)$
15	4	1	$\gcd(3, 15) = 3$
21	5	2	$\gcd(3, 21) = 3$
35	6	1	$\gcd(5, 35) = 5$
91	10	3	$\gcd(7, 91) = 7$
8	3	1	$\gcd(2, 8) = 2$

In each case $x^2 - y^2$ is a multiple of n while neither $x - y$ nor $x + y$ is, and (as in the daily post due Sept 18) the gcd hands you a factor.

What is special about these n

Observation: it never works for a prime, and it always works for a number with two different prime factors.

Primes are hopeless. If $n = p$ is prime and $x^2 \equiv y^2$, then $p \mid (x-y)(x+y)$, and since p is prime it divides one of the factors (Euclid's lemma). So $x \equiv y$ or $x \equiv -y$: the condition $x \not\equiv \pm y$ can never be met. Equivalently, every nonzero residue modulo a prime has exactly two square roots.

Two distinct prime factors always work. Say $n = ab$ with $\gcd(a, b) = 1$ and $a, b > 2$. By the Chinese remainder theorem choose x with

$$x \equiv 1 \pmod{a}, \qquad x \equiv -1 \pmod{b}.$$

Then $x^2 \equiv 1 \pmod{n}$, so take $y = 1$. And $x \not\equiv \pm 1 \pmod{n}$, because $x \equiv 1$ would force a and b both to divide $x - 1$, but $b \mid x + 1$ and $b \nmid 2$; similarly for -1. For $n = 15$, $a = 3$, $b = 5$, this recipe gives $x = 4$: indeed $4^2 = 16 \equiv 1$.

The exact rule. Restricting to x, y coprime to n (which is the useful case), such a pair exists precisely when the unit group $(\mathbb{Z}/n\mathbb{Z})^*$ is **not cyclic**, that is, for every n *except*

$$n = 1,\ 2,\ 4,\ p^k,\ 2p^k \qquad (p \text{ an odd prime}).$$

This was checked by machine for all $n < 300$. The reason: $x^2 \equiv y^2$ with x, y units is the same as $(xy^{-1})^2 \equiv 1$, so we are asking for a square root of 1 other than ± 1, and a cyclic group has exactly two elements of order dividing 2.

The practical summary for factoring: **if n has at least two distinct prime factors, such pairs exist, and each one factors n**; if n is prime, none exist (which is a primality test in disguise — this is what Miller-Rabin exploits); the remaining cases p^k and $2p^k$ are exactly the ones where the trick alone cannot separate the prime powers, though non-unit choices like $x = 2p, y = p$ modulo p^2 still reveal p through the gcd.

Problem 5: the Ceres birthday problem

The length of the Ceres year. Ceres orbits the Sun in about 4.60 Earth years, which is

$$N \approx 1682 \text{ Earth days}$$

(the usual figure is 1681.63 days). A "Ceres birthday" is one of these N equally likely days.

The approximation formula. With N equally likely birthdays and m people, the probability of no shared birthday is approximately

$$\Pr[\text{no collision}] \approx e^{-m(m-1)/(2N)} \approx e^{-m^2/(2N)}.$$

Setting this equal to $1/2$ and solving:

$$e^{-m^2/(2N)} = \tfrac{1}{2} \implies \frac{m^2}{2N} = \ln 2 \implies m = \sqrt{2N \ln 2} \approx 1.1774\sqrt{N}.$$

Plugging in.

$$m \approx 1.1774\sqrt{1682} = 1.1774 \times 41.01 \approx 48.3.$$

Rounding up, **49 people** are needed for at least a 50% chance of a shared Ceres birthday.

Check. The exact computation, multiplying out $\prod_{i=0}^{m-1}(1 - i/N)$, first drops below $1/2$ at $m = 49$ as well (the exact probability is 0.4930 at $m = 49$ and 0.5075 at $m = 48$ for no-collision, i.e. collision probability 0.5070 at $m = 49$). The answer is insensitive to the exact orbital period: $N = 1681$, 1682 or 1683 all give 49.

A remark on the rule of thumb from class. In lecture the cutoff was quoted as "$r^2/2N$ around 0.8". That is the same estimate with a little safety margin: $r = \sqrt{1.6N} = 1.265\sqrt{N}$ gives $r \approx 52$ here. Solving exactly, $r^2/2N = \ln 2 = 0.693$, gives 48.3, and the exact product formula confirms 49. Any answer in the high forties, with the reasoning shown, is right.

Moral. The count grows like $\sqrt{N}$, not like N: a Ceres year is about 4.6 times longer than an Earth year, but the number of people needed only grows by about $\sqrt{4.6} \approx 2.1$, from 23 to 49. This square-root behaviour is exactly what makes birthday attacks (collision attacks on hash functions, the baby-step giant-step algorithm, Pollard rho) so much cheaper than brute force.

Problem 6: Fermat's primality test on 2001 and 2003

Recall the test: if n is prime and $\gcd(a, n) = 1$, then Fermat's little theorem says $a^{n-1} \equiv 1 \pmod{n}$. So if we find $a^{n-1} \not\equiv 1 \pmod{n}$, the number n is **definitely composite** (a is then called a *Fermat witness* for n); if $a^{n-1} \equiv 1$, then n is only **probably prime**, and a has been fooled.

$n = 2001$, base $a = 2$

We need $2^{2000} \bmod 2001$. Write 2000 in binary: $2000 = 11111010000_2 = 1024 + 512 + 256 + 128 + 64 + 16$. Successive squaring modulo 2001:

k	$2^k \bmod 2001$	
1	2	
2	4	
4	16	
8	256	
16	1504	$*$
32	886	
64	604	$*$
128	634	$*$
256	1756	$*$
512	1996	$*$
1024	25	$*$

(each line is the square of the previous one, reduced; the starred lines are the powers of two appearing in 2000). Multiplying the starred entries modulo 2001:

$$2^{2000} \equiv 1504 \cdot 604 \cdot 634 \cdot 1756 \cdot 1996 \cdot 25 \equiv \mathbf{1225} \pmod{2001}.$$

Since $1225 \neq 1$, **2001 is composite**, and we know this without having found a factor. (For the record, $2001 = 3 \cdot 23 \cdot 29$.)

$n = 2003$, base $a = 2$

Now $2002 = 11111010010_2 = 1024 + 512 + 256 + 128 + 64 + 16 + 2$, and squaring modulo 2003:

k	$2^k \bmod 2003$	
1	2	
2	4	$*$
4	16	
8	256	
16	1440	$*$
32	495	
64	659	$*$
128	1633	$*$
256	696	$*$
512	1693	$*$
1024	1959	$*$

The product of the starred entries is $2^{2002} \equiv \mathbf{1} \pmod{2003}$. So **2003 is probably prime**: the test did not detect compositeness.

Trying a different base, as asked

Since 2003 came up probably prime, try $a = 3$. The same exponent 2002 and the same starred positions, now modulo 2003: $3, 9^*, 81, 552, 248^*, 1414, 402^*, 1364^*, 1712^*, 555^*, 1566^*$, whose starred product is

$$3^{2002} \equiv \mathbf{1} \pmod{2003}.$$

So 3 also says probably prime.

What we learn. Each new base that returns 1 is more evidence, but never a proof. Two things can be happening:

- n really is prime (true here: 2003 is prime), or
- n is a *Fermat pseudoprime* to the bases we tried. Some composites fool many bases; the **Carmichael numbers** ($561 = 3 \cdot 11 \cdot 17$, 1105, 1729, 2465, 2821, 6601, ...) fool *every* base coprime to n, so no amount of Fermat testing will ever detect them.

This is exactly why we go on to the Miller-Rabin test, which also looks at the square roots of 1 encountered along the way and so cannot be fooled by Carmichael numbers.

For contrast, the composite 2001 was caught by the very first base. Trying $a = 3$ on 2001 gives $3^{2000} \equiv 915 \pmod{2001}$ — also not 1, another witness. Most bases are witnesses for a typical composite; it is only the rare pseudoprimes that require care.