Numbers for Masochists: A Mental Factoring Cheat Sheet

by Richard Schroeppel and Hilarie Orman

Full paper at http://www.purplestreak.com/g4g13/mentalfactoring.pdf

Quick divisibility tests
2: low order digit of n is even. **3**: sum of the digits of n is divisible by 3.
5: low order digit is zero or 5. **7**: if $n = abc$, then n modulo 7 is $2 * a + bc$.
7, 11, and 13: $abcd$ modulo 1001 is $bcd - a$.
11: For abc, if $b = a + c$ or $b + 11 = a + c$, then $abc = 11 * ac$ or $11 * zc$ where $z = a - 1$. $11|abcd$ iff $a + c$ and $b + d$ are equal or if the difference is 11. **13**: $n/300 = \{q, r\}$, $13|(q + r)$ iff $13|n$.
37: If n has 3 digits, rotation preserves divisibility by 37.
97, 101, 103, . . .: each $100 \pm n$ divides $10000 - n^2$.

Table 1: Useful and Memorable Multiples of Small Primes

	Column - high order digits, Row - units digit			
	1	3	7	9
1	1001	299, 1001	102, 1003, 6001, 10013	399, 1007, 1501, 7999, 10013
2		2001		2001
3	992, 3999, 10013		111, 999	
4	10004	301, 3999, 10019	10011	
5		1007, 10017		1003, 20001
6	10004		201	
7	994, 10011	511, 1022, 10001		1501, 3002
8		996, 20003		801
9			9991	
10	9999	9991	9951, 20009	981, 10028, 40003
11		1017, 20001		
12			1016, 8001	
13			10001	
24	964, 20003			

The Method for Factoring n: Using Table 2, select the quadratic form(s) and the term that is divisible by 5 (NB: if there is no entry for n, use the 120 Method and/or Difference of Squares). Solve each form modulo 100 using the fact that one of the squares is a multiple of 25. For each form, there will be one or two solutions < 25, call them r (and s). The candidates for the non-multiple-of-5 term are the set $\{50i \pm r, 50i \pm s\}$ such that the square is less than n (or $n/2$ or $n/3$).

For each candidate value, plug in its square into the quadratic form and solve for the square of the other variable. If that solution is, indeed, a square, and if $\gcd(x, y) = 1$, then the x and y values are a solution to the quadratic form.

If you find **two solutions**, the number is composite. Calculate the factors using vector addition/subtraction on the two solutions to minimize the result vector (u, v) and/or to have both terms divisible by 5. Divide both terms by $\gcd(u, v)$. Substitute u and v for x and y in the QF; the result will have a factor of n.

If all potential candidates less than the square root of n have been tried, and there is only **one solution**, then n is prime. If there are **no solutions**, n is composite; the factorization must be done with another method.

Example: 4469. Per table 2, we use the QF $x^2 + y^2$. Either $x^2 \equiv 0 \mod 100$ or $x^2 \equiv 25 \mod 100$. First assume 0 mod 100; then $r = 13$ because $13 * 13 \equiv 69 \mod 100$. The y candidates are $50j \pm 13$, and $y < 70$. Possibilities are 13, 37, and 63.

$4469 - 13^2 = 4300$ which is not a square.

$4469 - 37^2 = 4469 - 1369 = 3100$ which is not a square.

$4469 - 63^2 = 4469 - 3969 = 500$ which is not a square. Therefore, $x^2 \equiv 0 \mod 100$ is impossible.

Now assume $x^2 \equiv 25 \mod 100$; find r such that $r^2 \equiv 69 - 25 \mod 100 = 44$. That would be 12. The y candidates are $50j \pm 12$, $y < 70$: 12, 38, and 62.

$4469 - 12^2 = 4325$ which is not a square because the hundreds digit is odd.

$4469 - 38^2 = 4469 - 1444 = 3025 = 55^2$. This is a representation of 4469 as $55^2 + 38^2$.

$4469 - 62^2 = 4469 - 3844 = 625 = 25^2$.

Table 2: Properties of quadratic form terms

residue	low digit	quadratic form	5 divides	x parity	y parity	r^2 mod 100
1 mod 4	1 or 9	$n = x^2 + y^2$	either	either	1-p(x)	n, $n - 25$
1 mod 4	3 or 7	$2n = x^2 + y^2$	either	odd	odd	$n - 25$
3 mod 8	1 or 9	$n = x^2 + 2y^2$	y	odd	odd	$n - 50$
		$3n = x^2 + 2y^2$	x	odd	even	$(3n - 25)/2$
3 mod 8	3 or 7	$n = x^2 + 2y^2$	x	odd	odd	$(n - 25)/2$
		$3n = x^2 + 2y^2$	y	odd	even	$3n$
7 mod 24	1 or 9	$n = x^2 + 3y^2$	y	even	odd	$n - 75$
		$4n = x^2 + 3y^2$	y	odd	odd	$4n - 75$
7 mod 24	3 or 7	$n = x^2 + 3y^2$	x	even	odd	$n/3$
		$4n = x^2 + 3y^2$	x	odd	odd	$(4n - 25)/3$

Add the two representations $(55, 38)$ and $(25, 62)$ to get $(80, 100)$. The gcd is 20, dividing it out yields $(4, 5)$, $4^2 + 5^2 = 41$. By mental arithmetic, $4469/41 = 109$.

Filters. $n \equiv x^2 + y^2 \mod 3$. The squares modulo 3 are 0 and 1, the corresponding square roots are 0, ± 1. Let m be the residue of n modulo 3. List all solutions to $m \equiv u^2 + v^2 \mod 3$ using 0 and 1 for u^2 and v^2. When trying an x or y candidate, check that it is consistent with the solution set modulo 3. If it isn't, discard it. You can do the same thing modulo 9 (squares are 0, 1, 4, and 7), modulo 7 (squares are 0, 1, 2, and 4), or modulo 49 (squares are 0, $7j + \{1, 2, 4\}$).

Modulo 100 filters. Match the parity of the hundreds digits in n and the square of a candidate value. If y is an odd multiple of 5 and the QF is $x^2 + 2y^2$, use the pattern of thousands-hundreds digits. If the QF is $x^2 + 3y^2$ and the tens digit of n is odd, match the parity of the hundreds digit of $n - 25$ or $n - 75$ to the parity of the hundreds digit of the candidate.

Example: $1000009 = 1000^2 + 3^2$. From Table 2, $y^2 \mod 100$ is either 00 or 25.
$09 - 00 = 9 = x^2 \mod 100 \rightarrow r = 3$, and $09 - 25 = 84 = x^2 \mod 100 \rightarrow r = 22$, so the x candidates are $50 + 3$, $50 - 3$, $50 - 22$, $50 + 22$, $\ldots$; 50 ± 22 is modified to 100 ± 28 to match hundred's digit parity. Squares modulo 9 eliminate 997; squares modulo 7 and modulo 9 accept 972. $1000009 - 972^2 = 55225 = 235^2$. Combine $(1000, 3)$ with $(235, 972)$ to get factors 293 and 3413.

The 120 Method. Find solutions to $kn = ax^2 + by^2$ where k, a, and b are small. For each solution, add $-ab$ to the set Q and compute the closure of Q under multiplication, exact division, and division by a square.
For a $4i + 3$ number, if 2, 3, and 5 (irrespective of sign) are in Q, n can be factored or proved prime. For a $4i + 1$ number, if -1, 2, 3, and 5 are in Q, n can be factored or proved prime.
The trial divisors of n for a $4i + 3$ number: $120j + \{1, 49, d, e\}$ where $d = n \mod 120$, $e = 60 - 11d \mod 120$ and j goes from 0 to $\sqrt{n}/120$; for a $4i + 1$ number: $120j + \{1, 49\}$ where j goes from 0 to $\sqrt{n}/120$. Only prime divisors need be tested.

Example 2503: $n = 50^2 + 3 = 51^2 - 98 = 15 * 13^2 - 32$. The corresponding $-ab$ values are -3, 2, 30. By closure, $Q = \{2, 3, 30, 15, 5\}$. Then $d = 103$, $e = 7$; trial divisors are $120j + \{1, 7, 49, 103\}$. Testing 7 fails, 49 is composite, $103 > \sqrt{n}$. Therefore n is prime.

The Difference of Squares Method. Find x and y such that $n = x^2 - y^2$. One of the two squares will end in 00 or 25. Solve for the other square modulo 100 using the following equations.
For $n \equiv 1 \mod 4$:
$x \equiv 5 \mod 10$, $y^2 \equiv 25 - n \mod 100$
$y \equiv 0 \mod 10$, $x^2 \equiv n + 0 \mod 100$
For $n \equiv 3 \mod 4$:
$x \equiv 0 \mod 10$, $y^2 \equiv 0 - n \mod 100$
$y \equiv 5 \mod 10$, $x^2 \equiv n + 25 \mod 100$

Of the two solutions, one is based on x, the other on y. Use the solutions to build candidate sets of the form $\{50j \pm r\}$ as in The Method; one is for x candidates, the other is for y candidates. Alternate trying x candidates and y candidates, then change the limits for x and y as described next. If x and y both exceed their limits, then n is prime.

Limits for x and y. Use divisibility tricks to eliminate possible divisors up to $L = 37$. Call the upper limit for x L_x. $L_x = (L + n/L)/2$; the upper limit for y is $L_x - L$. To change the limits, use mental arithmetic to test more primes in sequence, set L to the last prime tested, and recompute the limits. Divisor restrictions (see full paper) can eliminate some primes without testing.