MATH 56 WORKSHEET : Quadratic sieve, Kraitchik

Bamett
5/14/13.

Use Kraitchik's method to factor $N=2041$, using factor base $\{2,3,5,7\}$:

A) $x = 46$ $\quad x^2 - N = 75$

prime factorization $= 2^0 \cdot 3^1 \cdot 5^2 \cdot 7^0$

[does it use only the factor base?]

Continue: [may use sage to help!]

$x = 47$ $\quad x^2 - N = \ldots$

48

49

50

51

Cross out the x's not lying in the factor base.

B) What u^2, product of some remaining x^2's, gives a perfect square v^2, mod N?

Compute $u \bmod N$, $v \bmod N$ & check $u \neq \pm v \bmod N$: [may use sage!]

C) Write a linear algebra criterion for finding a perfect square: [Hint: make a matrix of factor base powers]

D) It's much easier if solve linear system mod something — what? Give the matrix.

MATH 56 WORKSHEET : Quadratic sieve; Kraitchik

Bennett 5/14/13.

SOLUTION

Use Kraitchik's method to factor $N=2041$, using factor base $\{2,3,5,7\}$:

A) $x = 46$ $\quad x^2 - N = 75$ $\quad$ prime factorization $= 2^0 \cdot 3^1 \cdot 5^2 \cdot 7^0$

[does it use only the factor base?]

Continue: [may use sage to help!]

$x = 47$ $\quad x^2 - N = 168$ $\quad 2^3 \cdot 3 \cdot 7$

~~48~~ $\quad$ 263 $\quad \rightarrow$ 263 prime!

49 $\quad$ 360 $\quad 2^3 \cdot 3^2 \cdot 5$

~~50~~ $\quad$ 459 $\quad 3^3 \cdot 17$

51 $\quad$ 560 $\quad 2^4 \cdot 5 \cdot 7$

Cross out the x's not lying in the factor base.

B) What u^2, product of some remaining x^2's, gives a perfect square v^2, mod N? (one multiple of each of 4 remaining rows.)

$$u^2 = (46 \cdot 47 \cdot 49 \cdot 51)^2 = 2^{10} \cdot 3^4 \cdot 5^4 \cdot 7^2$$

$u = 46 \cdot 47 \cdot 49 \cdot 51 = 5402838$ $\quad$ $v = 2^5 \cdot 3^2 \cdot 5^2 \cdot 7 = 50400$

Compute $u \bmod N$, $v \bmod N$ & check $u \neq \pm v \bmod N$: [may use sage!]

311 $\quad$ 1416 $\quad$ & true. $\quad$ so factors

$\gcd(u \pm v, N) = 13, 157$

C) Write a linear algebra criterion for finding a perfect square: [Hint: make a matrix of factor base powers]

$[a_1\ a_2\ a_3\ a_4] \begin{bmatrix} 0 & 1 & 2 & 0 \\ 3 & 1 & 0 & 7 \\ 3 & 2 & 5 & 0 \\ 4 & 0 & 1 & 1 \end{bmatrix} =$ [row of even #s]

$x_1 = 46$ 47 49 51

fb: 2 3 5 7

$[1\ 1\ 1\ 1] \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$

a left null vector mod 2.

D) It's much easier if solve linear system mod something — what? Give the matrix.

↳ mod 2.