Example of Quadratic Residues Contd.

Let *m be a positive integer and a any integer such that (a, m)= 1. Then a is a* quadratic residue of *m if the congruence* $x^2 \equiv a \pmod{m}$ *is solvable; otherwise,* it is a quadratic nonresidue of *m*.

Find the quadratic residues and non-residues of $p = 13$.

Example of Quadratic Residues Contd.

Find the quadratic residues and non-residues of $p = 13$.

SOLUTION

Notice that

$1^2 \equiv 1 \equiv 12^2 \pmod{13}$ $\quad$ $2^2 \equiv 4 \equiv 11^2 \pmod{13}$

$3^2 \equiv 9 \equiv 10^2 \pmod{13}$ $\quad$ $4^2 \equiv 3 \equiv 9^2 \pmod{13}$

$5^2 \equiv 12 \equiv 8^2 \pmod{13}$ $\quad$ $6^2 \equiv 10 \equiv 7^2 \pmod{13}$

Accordingly, 13 has exactly six quadratic residues, namely, 1, 3, 4, 9, 10, and 12; and it has six quadratic nonresidues also, namely, 2, 5, 6, 7, 8, and 11

Quadratic Residues

We begin by considering the quadratic congruence

$Ax^2 + Bx + C \equiv 0 \pmod{p}$...1

where *p is an odd prime and p does not divides A. (If p|A, then it reduces to a linear congruence.)*

Since *p is odd and p does not divides A, p does not divides 4A. So we multiply both sides of congruence equation 1 by 4A to yield a perfect square on the LHS:*

$4A(Ax^2 + Bx + C) \equiv 0 \pmod{p}$..2

But $4A(Ax^2 + Bx + C) = 4A^2x^2 + 4ABx + 4AC$

$= (2Ax + B)^2 - B^2 + 4AC$

Quadratic Residues Contd.

Therefore, congruence equation 2 can be rewritten as

$(2Ax + B)^2 \equiv B^2 - 4AC \pmod{p}$.......................................3

which is of the form $y^2 \equiv a \pmod{p}$.................................4

where $y = 2Ax + B$ *and* $a = B^2 - 4AC$.

Since these steps are reversible, this discussion shows that congruence equation-1 is solvable if and only if congruence equation-4 is solvable.

Example of Quadratic Residues Contd.

Solve the quadratic congruence $3x^2 - 4x + 7 \equiv 0 \ (mod 13)$.

Example of Quadratic Residues Contd.

Solve the quadratic congruence $3x^2 - 4x + 7 \equiv 0 \pmod{13}$.

SOLUTION

$$3x^2 - 4x + 7 \equiv 0 \pmod{13}$$

Multiply both sides by $4 \cdot 3 = 12$:

$$36x^2 - 48x + 84 \equiv 0 \pmod{13}$$

That is,

$$(6x - 4)^2 \equiv (16 - 84) \pmod{13}$$

$$(6x - 4)^2 \equiv 10 \pmod{13}$$

Let $y = 6x - 4$. Then $y^2 \equiv 10 \pmod{13}$. *This congruence has exactly two solutions,* $y \equiv 6, 7 \pmod{13}$. *(Verify this.)*

Therefore, the solutions of the congruence are given by those of the linear congruences $6x - 4 \equiv 6 \pmod{13}$ *and* $6x - 4 \equiv 7 \pmod{13}$, *namely,* $x \equiv 6, 4 \pmod{13}$.

Example of Quadratic Residues Contd.

Every odd prime p has exactly (p−1)/2 quadratic residues and (p−1)/2 quadratic nonresidues.

Example of Quadratic Residues Contd.

Let ‘p’ be an odd prime. *Then a positive integer ‘a’ with ‘p’ does not divide ‘a’ is a* quadratic residue of *p if and only if* $a^{(p-1)/2} \equiv 1 \pmod{p}$.

Example of Quadratic Residues Contd.

Let ‘p’ be an odd prime. *Then a positive integer ‘a’ with ‘p’ does not divide ‘a’ is a* quadratic residue of *p if and only if* $a^{(p-1)/2} \equiv 1 \pmod{p}$.

Example of Quadratic Residues Contd.

- Determine whether 10 and 7 are quadratic residues of 13.

- *Notice that* $10^{(13-1)/2} = 10^6 \equiv 1 \pmod{13}$*, so, by Euler's criterion, 10 is a quadratic residue of 13, (Consequently, the congruence* $x^2 \equiv 10 \pmod{13}$ *is solvable.)*

- Compute $7^{(13-1)/2} \pmod{13}$: $7^{(13-1)/2} \equiv 7^6 \equiv 12 \pmod{13}$. *Since* $7^6 \equiv 12 \pmod{13}$*, by Euler's criterion, 7 is a quadratic* Non-residue of 13.

Smooth numbers

Definition. An integer *n is called B-smooth if all of its prime factors are less* than or equal to *B*.

Example. Here are the first few 5-smooth numbers and the first few numbers that are not 5-smooth:

5-smooth	:	*2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 16, 18, 20, 24, 25, 27, 30,32, 36, . . .*
Not 5-smooth	:	*7, 11, 13, 14, 17, 19, 21, 22, 23, 26, 28, 29, 31, 33, 34, 35, 37, . . .*

Smooth numbers

Definition. The function *$\psi(X, B)$ counts B-smooth numbers,* *$\psi(X,B)$ = Number of B-smooth integers n such that $1 < n \leq X$.*

For example, $\psi(25, 5) = 15$,

Since the 5-smooth numbers between 1 and 25 are the 15 numbers 2, *3, 4, 5, 6, 8, 9, 10, 12, 15, 16, 18, 20, 24, 25.*

Smooth numbers

- A **smooth number** is an integer whose prime factors are less or equal to a prescribed bound (**smoothness bound**).
- If this bound is B, we can say that the number is B-smooth.
- For example the number 900 is **10-smooth, because** $900 = 2^2 \times 3^2 \times 5^2$
- Its greatest prime factor is 5, and 5 <= 10.

Quadratic Sieve (QS),

The Quadratic Sieve (QS), invented by Pomerance (then at the University of Georgia) in 1981 and first published in 1982 [245], belongs to a wide range of factoring algorithms, called index calculus of factoring, along with Continued fraction method (CFRAC) [223] and Number Field Sieve (NFS) [187]; all of them make use of the simple but important observation that if we have two integers *x and y such that*

$$x^2 \equiv y^2 \pmod{N},\ 0 < x < y < N,\ x \neq y,\ x + y \neq N, \tag{3.1}$$

then $\gcd(x \pm y,\ N)$ are possibly the nontrivial factors of N, because $N \mid (x+y)(x-y)$, but $N \nmid (x+y)$ and $N \nmid (x-y)$. For example, to factor $N = 8051$, we find $90^2 \equiv 7^2 \pmod{N}$, hence $\gcd(90 \pm 7,\ N) = (97, 83)$, thus $8051 = 83 \cdot 97$. How to find the x and y such that the congruence (3.1) is satisfied is the main task of the index calculus; different methods use different techniques to find such pairs of (x, y). A version of QS may be described as follows:

Quadratic Sieve (QS) Algorithm

[1] (Factor Base) Define a factor base as follows:

$$\mathrm{FB} = \{-1, p_1, p_2, \cdots, p_k \leq B\}$$

where p_i are primes for which N is a quadratic residue modulo p_i, and B is the upper bound of the factor base (the largest prime in the factor base).

[2] (Smoothness) Find $a_1, a_2, \cdots, a_k$, close to $\sqrt{N}$ (this can be done via e.g., $a_i = \lfloor\sqrt{N}\rfloor + 1, \lfloor\sqrt{N}\rfloor + 2, \cdots, (N-1)/2$) such that each $Q(a_i) = a_i^2 - N$ is smooth (a number is smooth if all its prime factors are small with respect to the bound B. In this case, the number is called B-smooth).

Quadratic Sieve (QS) Algorithm Contd.

[3] (Linear Algebra – Finding $x^2 \equiv y^2 \pmod{N}$) Use linear algebra to find a subset U of the numbers $Q(a_i) = a_i^2 - N$ whose product $\prod p_i^{\alpha_i}$ is a square, say $y^2 \bmod N$. That is, $y^2 \equiv \prod a_i^2 - N$. Let x be the product a_i used to form the square, modulo N. Then

$$\begin{aligned}
x^2 &\equiv \left(\prod_{i \in U} a_i\right)^2 \\
&\equiv \prod_{i \in U} (a_i^2 - N) \\
&\equiv \prod_{i \in U} Q(a_i) \\
&\equiv \left(\prod_{i \in U} p_j^{\alpha_{j,i}}\right)^2 \\
&\equiv y^2 \qquad\qquad \pmod{N}.
\end{aligned}$$

Quadratic Sieve (QS) Algorithm Contd.

[4] (Computing GCD) $(f, g) = \gcd(x \pm y, N)$.

[5] (OK?) If $1 < f, g < N$, print (f, g) (in terms of RSA, (f, g) will be the prime factors (p, q) of the modulus N) and go to [6]. Otherwise, go to [3] to find new x and y and. If necessary, go to [2] to find more a_i's.

[6] Exit.

Quadratic Sieve (QS) Algorithm Contd.

Example 3.4.1. Use Algorithm 3.4.1 to factor $N = 1829$.

[1] (Factor Base) Let the factor base be as follows:

$$\text{FB} = \{-1, 2, 5, 7, 11\}.$$

Note although $3 < 11$ is a prime but for which N is not a quadratic residue, so we exclude it from the factor base.

[2] (Smoothness) Choose $a_i \sim \lfloor\sqrt{1829}\rfloor = 29$. Let $a_i = 27, 28, 29, \cdots$, compute $Q(a_i) = a_i^2 - N$, keep only the smooth $Q(a_i)$, and get the corresponding exponent vectors modulo 2 as follows:

Quadratic Sieve (QS) Algorithm Contd.

$$
\begin{array}{lllcccccc}
 & & & & -1 & 2 & 5 & 7 & 11 \\
1) & Q(27) = 27^2 - N = -1100 = -2^2 \cdot 5^2 \cdot 11 & \longleftrightarrow & (& 1, & 0, & 0, & 0, & 1) \\
2) & Q(38) = 38^2 - N = -385 = -5 \cdot 7 \cdot 11 & \longleftrightarrow & (& 1, & 0, & 1, & 1, & 1) \\
3) & Q(39) = 39^2 - N = -308 = -2^2 \cdot 7 \cdot 11 & \longleftrightarrow & (& 1, & 0, & 0, & 1, & 1) \\
4) & Q(43) = 43^2 - N = 20 = 2^2 \cdot 5 & \longleftrightarrow & (& 0, & 1, & 1, & 0, & 0) \\
5) & Q(45) = 45^2 - N = 196 = 2^2 \cdot 7^2 & \longleftrightarrow & (& 0, & 0, & 0, & 0, & 0) \\
6) & Q(52) = 52^2 - N = 875 = 5^3 \cdot 7 & \longleftrightarrow & (& 0, & 0, & 1, & 1, & 0) \\
7) & Q(53) = 53^2 - N = 980 = 2^2 \cdot 5 \cdot 7^2 & \longleftrightarrow & (& 0, & 0, & 1, & 0, & 0)
\end{array}
$$

Quadratic Sieve (QS) Algorithm Contd.

[3] (Linear Algebra – Finding $x^2 \equiv y^2 \pmod{N}$) Use linear algebra to find a subset of the numbers $Q(a_i) = a_i^2 - n$ whose product $\prod p_i^{\alpha_i}$ is a square; if the sum of the corresponding exponent vectors modulo 2 is zero, then the subset of the numbers $Q(a_i)$ form a square. Observe that (this can be done systematically) the sum of the first, the second and the sixth vectors is zero. That is,

$$\begin{array}{rcl} & (1,0,0,0,1) & \text{1st} \\ & (1,0,1,1,1) & \text{2nd} \\ \oplus & (0,0,1,1,0) & \text{6th} \\ \hline & (0,0,0,0,0,0) & \Longrightarrow \text{Successful} \end{array}$$

Quadratic Sieve (QS) Algorithm Contd.

So, we have found a suitable pair of (x, y), which produce squares in both sides $(27 \cdot 38 \cdot 52)^2 \equiv (2 \cdot 5^3 \cdot 7 \cdot 11)^2$. Thus, we have

$$
\begin{aligned}
x &= 27 \cdot 38 \cdot 52 \\
&= 53352 \\
&\equiv 311 \pmod{1829} \\
y &= 2 \cdot 5^3 \cdot 7 \cdot 11 \\
&= 19250 \\
&\equiv 960 \pmod{1829}.
\end{aligned}
$$

Quadratic Sieve (QS) Algorithm Contd.

Note that some other subsets of the number $Q(a_i)$ such as the 2nd, 3rd and 7th also form a square:

$$
\begin{array}{rccc}
 & (1,0,1,1,1) & & \text{2nd} \\
 & (1,0,0,1,1) & & \text{3rd} \\
\oplus & (0,0,1,0,0) & & \text{7st} \\
\hline
 & (0,0,0,0,0,0) & \Longrightarrow & \text{Successful}
\end{array}
$$

That is, $(38 \cdot 39 \cdot 53)^2 \equiv (2^2 \cdot 5 \cdot 7^2 \cdot 11)^2$. Thus,

$$
\begin{aligned}
x &= 38 \cdot 39 \cdot 53 \\
&= 78546 \\
&\equiv 1728 \pmod{1829} \\
y &= 2^2 \cdot 5 \cdot 7^2 \cdot 11 \\
&= 10780 \\
&\equiv 1635 \pmod{1829}.
\end{aligned}
$$

Quadratic Sieve (QS) Algorithm Contd.

[4] (Computing GCD) Compute $(f,g) = \gcd(x \pm y, N)$, and hopefully, (f,q) will be the required prime factors (p,q) of N. Since we have found two pairs of

$$(x,y) = (311, 960) = (1728, 1635).$$

Thus we have

$$(f,g) = \gcd(x \pm y, N) = \gcd(311 \pm 960, 1829) = (31, 59).$$

That is, $1829 = 31 \cdot 59$. Alternatively, we have

$$(f,g) = \gcd(x \pm y, N) = \gcd(1728 \pm 1635, 1829) = (59, 31).$$

That is, $1829 = 59 \cdot 31$.