Sketch of Lecture 12 Mon, 2/6/2017

Definition 73. An integer a is a **quadratic residue** modulo n if $a \equiv x^2 \pmod{n}$ for some x.

Example 74. List all quadratic residues modulo 11.

Solution. We compute all squares: $0^2 = 0$, $(\pm 1)^2 = 1$, $(\pm 2)^2 = 4$, $(\pm 3)^2 = 9$, $(\pm 4)^2 \equiv 5$, $(\pm 5)^2 = 3$. Hence, the quadratic residues modulo 11 are $0, 1, 3, 4, 5, 9$.

Important comment. Exactly half of the 10 nonzero residues are quadratic. Can you explain why?

[*Hint.* If $x^2 \equiv y^2 \pmod{p}$ or, equivalently, $(x - y)(x + y) \equiv 0 \pmod{p}$, then $x \equiv y$ or $x \equiv -y \pmod{p}$.]

Example 75. List all quadratic residues modulo 15.

Solution. We compute all squares: $0^2 = 0$, $(\pm 1)^2 = 1$, $(\pm 2)^2 = 4$, $(\pm 3)^2 = 9$, $(\pm 4)^2 \equiv 1$, $(\pm 5)^2 = 10$, $(\pm 6)^2 = 6$, $(\pm 7)^2 = 4$. Hence, the quadratic residues modulo 15 are $0, 1, 4, 6, 9, 10$.

Important comment. Among the $\varphi(15) = 8$ invertible residues, the quadratic ones are $1, 4$ (exactly a quarter). Can you give a reason why this is to be expected?

[*Hint.* Note that 15 is of the form $n = pq$ with p, q distinct primes. By the Chinese Remainder Theorem (review!), a is a quadratic residue modulo $n = pq$ if and only if a is a quadratic residue both modulo p and modulo q. Since half of the residues are quadratic modulo a prime, we expect that a is a quadratic residue modulo both primes with probability $\frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$. The bonus challenge below asks to make that precise.]

Example 76. (bonus challenge) Give a precise reason (i.e. prove) why, if $n = pq$ with p, q distinct primes, exactly a quarter of all invertible residues are quadratic.

[*Hint.* Start again with $x^2 \equiv y^2 \pmod{n}$, ... Alternatively, use the Chinese Remainder Theorem.]

The following is an example of a PRG, which is believed to be unpredictable.

More precisely, it has been shown that the ability to predict its values is equivalent to being able to efficiently solve the quadratic residuosity problem (which is believed to be hard). Currently, the best way to "solve" the quadratic residuosity problem mod M relies on factoring M. However, factoring large numbers is considered to be hard, see Example 78 (and lots of crypto relies on that).

Quadratic residuosity problem. Given big $M = pq$ and a residue x modulo M, decide whether x is a quadratic residue. (About $M/4$ are quadratic residues (see above); $M/2$ are easily determined to be nonsquare using the Jacobi symbol [don't worry if you haven't heard about that].)

(Blum-Blum-Shub PRG) Let $M = pq$ where p, q are large primes $\equiv 3 \pmod{4}$.
From the seed y_0 (needs to be coprime to M), we generate $y_{n+1} = y_n^2 \pmod{M}$.
The random bits we produce are $x_n = \text{least bit of}(y_n)$.

BBS is very slow, and mostly of theoretical value. However, as mentioned above, it is interesting because it is indeed unpredictable if an important number theory problem is "hard" (this can be made precise), as is believed to be the case.

Why the conditions on p and q? Recall from the CRT that an invertible quadratic residue x^2 modulo $M = pq$ has exactly four squareroots $\pm x$, $\pm y$. The condition $3 \pmod{4}$ guarantees that, of these four, exactly one is itself a quadratic residue. As a consequence, the mapping $y \mapsto y^2 \pmod{M}$ is 1-1 when restricted to invertible quadratic residues (see Example 80).

Comment. To increase speed, at the expense of some security, we can also take several, say k, bits of y_n (as long as k is small, say, $k \leqslant \log_2 \log_2 M$).

Example 77. Generate random bits using the B-B-S PRG with $M=77$ and seed 3.

Solution. With $y_0=3$, we have $y_1=y_0^2=9$, followed by $y_2=y_1^2\equiv 4 \pmod{77}$, $y_3\equiv 16$, $y_4\equiv 25$, $y_5\equiv 9$, so that the values y_n now start repeating.

These numbers are, however, not the output of the PRG. We only output the least bit of the numbers y_n, i.e. the value of $y_n \pmod{2}$. For $y_1\equiv 9$ we output 1, for $y_2\equiv 4$ we output 0, for $y_3\equiv 16$ we output 0, for $y_4\equiv 25$ we output 1, and so on.

In other words, the seed 3 produces the sequence $1,0,0,1,1,0,0,1,1,0,\ldots$ of period 4.

Comment. Note that it was completely to be expected that the numbers repeat. In fact, we immediately see that the number of possible y_n is at most the number of invertible quadratic residues, of which [by the previous example] there are only $\phi(77)/4=15$. See Example 104 for a better prediction.

Example 78. We mentioned that the unpredictability of the B-B-S PRG relies on the difficulty of factoring large numbers. Here's an indication how difficult it seems to be. In 1991, RSA Laboratories challenged everyone to factor several numbers including:

1350664108659952233496032162788059699388814756056670275244851438515265\
1060485953383394028715057190944179820728216447155137368041970396419174\
3046496589274256239341020864383202110372958725762358509643110564073501\
5081875106765946292055636855294752135008528794163773285339061097505443\
34999811150056977236890927563

Since then, nobody has been able to factor this 1024 bit number (309 decimal digits). Until 2007, cash prizes were offered up to 200,000 USD, with 100,000 USD for the number above.

https://en.wikipedia.org/wiki/RSA_Factoring_Challenge

Example 79. (homework) Generate random bits using the B-B-S PRG with $M=209$ and seed 10. What is the period of the generated sequence? (Then repeat with seed 25.)

Solution. (final answer only) The seed 10 produces the sequence $0,1,0,1,1,1,\ldots$ of period 6.

The seed 25 generates the sequence $1,0,0,1,1,0,1,0,0,0,1,1,\ldots$ of period 12.

[By the way, it is perfectly fine, and actually a great idea, to let Sage assist you.]

Example 80. (homework)

(a) List all invertible quadratic residues modulo 21. Then (as in B-B-S) compute the square of all these residues.

(b) Repeat the first part modulo 33 and modulo 35. When computing the squares of these, do you notice a difference modulo 35?

[Note that $35=5\cdot 7$ with $5\equiv 1 \pmod{4}$. This example illustrates an indication why these cases are excluded in B-B-S.]

(c) How many invertible quadratic residues are there modulo 707?

Solution. (final answers only)

(a) Among the $\phi(21)=12$ many invertible elements, the squares are $1,4,16$ (exactly a quarter).
Computing the squares: $1^2\equiv 1$, $4^2\equiv 16$, $16^2\equiv 4 \pmod{21}$. Note that the squares are all different!

(b) Modulo 33: among the $\phi(33)=20$ many invertible elements, the squares are $1,4,16,25,31$ (exactly a quarter). Computing the squares: $1^2\equiv 1$, $4^2\equiv 16$, $16^2\equiv 25$, $25^2\equiv 31$, $31^2\equiv 4 \pmod{33}$. Again, all the squares are different!

Modulo 35: among the $\phi(35)=24$ many invertible elements, the squares are $1,4,9,11,16,29$ (exactly a quarter). Computing the squares: $1^2\equiv 1$, $4^2\equiv 16$, $9^2\equiv 11$, $11^2\equiv 16$, $16^2\equiv 11$, $29^2\equiv 1 \pmod{35}$. Observe that these are not all different: for instance, $9^2\equiv 16^2 \pmod{35}$.

(c) $\frac{1}{4}\phi(707)=150$