# MODULAR SQUARE ROOTS

- **Square Roots mod m:** For $x, a, m$ integers and $m > 0$, $x$ is a square root of $a$ mod $m$ provided $x^2 \equiv a$ mod $m$.

- **Dan Shanks' observation about square roots mod p:**

  ♠ $p$ an odd prime $\Rightarrow p - 1 = s \cdot 2^e$ with $s$ odd and $e > 0$.

  ♠ $x = a^{(s+1)/2} \Rightarrow x^2 \equiv a^{s+1} \equiv a^s \cdot a \pmod{p}$

  ♠ $a^{(s+1)/2}$ is *almost* the square root of $a \pmod{p}$

  ♠ $a^s \equiv 1 \pmod{p} \Rightarrow a^{(s+1)/2}$ *is* the square root of $a \pmod{p}$ (two–thirds of the time, even!)

  ♠ $a^s \pmod{p}$ is a $2^e$th root of unity $\pmod{p}$

  ♠ $a^s \pmod{p}$ is a fudge factor which can be updated.

- **The Shanks–Tonelli algorithm:** It updates both the initial guess $x$ and the fudge factor $a^s$ until the f.f. $\equiv 1 \pmod{p}$.

# THE SHANKS–TONELLI ALGORITHM

**1. BEGIN** with an integer $a$ and a prime $p > 2$, relatively prime to $a$. Calculate $a^{(p-1)/2} \pmod{p}$. Now $a^{(p-1)/2} \equiv 1$ or $-1 \pmod{p}$.

**2. IF** $a^{(p-1)/2} \equiv -1 \pmod{p}$, then $a$ has no square root $\pmod{p}$. Say so, and **EXIT** quietly.

**3. IF** $a^{(p-1)/2} \equiv 1 \pmod{p}$, then we're in business. Write $p - 1 = s \cdot 2^e$ with $s$ odd and $e$ positive.

**4. FIND** a number $n$ such that $n^{(p-1)/2} \equiv 1 \pmod{p}$—that is, a nonsquare $\pmod{p}$.

**5. INITIALIZE** these variables (all congruences are mod $p$):

$x \equiv a^{(s+1)/2}$ (first guess at the square root)
$b \equiv a^s$ (first guess at the fudge factor)
$g \equiv n^s$ (powers of $g$ will update both $x$ and $b$)
$r = e$ (exponent will decrease with each update of the algorithm).
Note that $x^2 \equiv ba \pmod{p}$.

Now: **WHILE** $m > 0$

**6. FIND** the least integer $m$ such that $0 \le m \le r-1$ and $b^{2^m} \equiv 1 \pmod{p}$. That is, find $m$ such that $\mathrm{ord}_p(b) = 2^m$.

**7. IF** $m = 0$, we're done. **RETURN** the value of $x$ and **EXIT** triumphantly.

**8. IF** $m > 0$**, UPDATE** the variables:

$$\begin{aligned}
&\text{replace } x \text{ by } x \cdot g^{2^{r-m-1}}\\
&\text{replace } b \text{ by } b \cdot g^{2^{r-m}}\\
&\text{replace } g \text{ by } g^{2^{r-m}}\\
&\text{replace } r \text{ by } m.
\end{aligned}$$

end **WHILE**

# WHY DOES IT TERMINATE?

♡ Old value of $b$ satisfies $b^{2^{m-1}} \not\equiv 1 \pmod{p}$, but …

♠ … new value of $b$ satisfies $b^{2^{m-1}} \equiv 1 \pmod{p}$, so:

♡ The value of $m$ decreases with each update.

♡ Reason: for old $b$, $m$ minimal $\Rightarrow b^{2^{m-1}} \equiv -1 \pmod{p}$

♡ Also, $g^{2^{r-1}} \equiv -1 \pmod{p}$

♡ Hence, $\left(b \cdot g^{2^{r-m}}\right)^{2^{m-1}} \equiv b^{2^{m-1}} g^{2^{r-1}} \equiv 1 \pmod{p}$

♡ But $b \cdot g^{2^{r-m}}$ is the new value of $b$ (see ♠)

♡ So, the new value of $m$ is less than the old value of $m$.

# AN EXAMPLE

# THE SQUARE ROOT OF 2 MOD 113

**SET UP:** $a = 2, p = 113, p - 1 = 7 \cdot 2^4, e = 4, s = 7, (p-1)/2 = 56, (s+1)/2 = 4$

**BEGIN:** $2^{56} \equiv 1 \pmod{113}$; we're in business.

**FIND** $n$**:** $3^{56} \equiv -1 \pmod{113}$, so $n = 3$.

**INITIALIZE:** $x = a^{(s+1)/2} = 2^4 \equiv 16 \pmod{113}$; $b = a^s = 2^7 \equiv 15 \pmod{113}$;

$g = n^s = 3^7 \equiv 40 \pmod{113}$;

$r = e = 4$.

**FIND** $\mathrm{ord}_p(b) = 2^m$: $b^2 = 225 \equiv -1, b^4 \equiv 1 \pmod{113}$. Hence $b^{2^2} \equiv 1 \pmod{113}$, and so $m = 2$.

$m \neq 0$, so **UPDATE:**

$x = xg^{2^{r-m-1}} = 16 \cdot 40^{2^{4-2-1}} = 16 \cdot 1600 \equiv 16 \cdot 18 \equiv 62 \pmod{113}$;

$b = bg^{2^{r-m}} = 15 \cdot 40^4 \equiv 15 \cdot (-15) \equiv 1 \pmod{113}$;

$g = g^{2^{r-m}} \equiv -15 \pmod{113}$;

$r = m = 2$.

Since $b = 1$, $\mathrm{ord}_p(b) = 1 = 2^0$; hence $m = 0$ and we're done: **RETURN** the current value of $x$, namely 62. Sure enough, $62^2 = 3844 = 2 + 34 \cdot 113 \equiv 2 \pmod{113}$, and so 62 is a square root of 2 mod 113.