**Solving** $x^2 \equiv a \pmod p$**.** [Note, if $2{\neq}p \not| a$, $p^i \mid d{=}x^2{-}a$, $y = [x{-}d/(2x)]_{p^{2i}}$, then $y^2 \equiv a \pmod{p^{2i}}$. $p{=}2$ needs $2^{i+1}|d$. And $a{\in}(Z^*_{2^k})^2$ iff $8|a{-}1$.] **Let** $t \stackrel{\text{df}}{=} (p{-}1)/2 = 2^k(2s{-}1)$, $(b^2/a)^{2^i}{\equiv}1{\equiv}{-}r^{2^i}$. (E.g., $i{=}k$, $b{=}a^s$, $r \in (\mathbb{Z}^*_p)^{2s-1} \setminus (\mathbb{Z}^*_p)^2$.) Then $(x^2/a)^{2^{i-1}}{\equiv}1$ for $x{=}b$ or $x{=}br$. Also, $2 \notin (\mathbb{Z}^*_p)^2$ if $k{=}1$. Indeed, $t!\,\prod_{i\le t}(-1)^i = \prod_{i\le t} i(-1)^i \equiv (\prod_{i\le t/2} 2i)\prod_{i<t/2}(p{-}(2i{+}1)) = (\prod_{i\le t/2} 2i)\prod_{i<t/2} 2(t{-}i)$ $= \prod_{i\le t} 2i = t!\,2^t$. So, $2^t \equiv (-1)^{t(t+1)/2} = (-1)^{(p^2-1)/8}$ which is $-1$ iff $p = \pm 3 \pmod 8$.

**Rational reconstruction.** Let $n, b, r', t', k, -s' \in \mathbb{N}^+$, (for $t'{<}0$ take $b'{=}n{-}b$); $r'{=}t'b{+}s'n{\le}k{<}n/t'$, $\gcd(s',t'){=}1$. Let $\{(r_i, s_i, t_i)\}_i \stackrel{\text{df}}{=}$ EEA$(n,b)$. For $j$ with $r_j{\le}k{<}r_{j-1}$, let $(r,s,t) \stackrel{\text{df}}{=} (r_j, s_j, t_j)$. Assume $t{<}0$. Then $(r',s',t'){=}(R,S,T) \stackrel{\text{df}}{=} (r_{j-1}, s_{j-1}, t_{j-1}){-}(r,s,t)q$, with $q$ such that $r{>}k{-}R{\ge}0$.

**Proof:** Note that $r'{-}R{<}r$, $T{>}0$. Combining $r{=}tb{+}sn$, $R{=}Tb{+}Sn$ gives $rT{-}Rt{=}n(sT{-}St){=}n$. Also, $n|(rt'{-}r't){=}n$, as $rt'{\le}kt'{<}n$, $|r't|{\le}k|t|{<}kn/r_{j-1}{<}n$. Same way, $(s'T{-}St')n{=}(r'T{-}Rt')$ and $r(r'T{-}Rt') = r'(Rt{+}n){-}R(r't{+}n) = (r'{-}R)n$. So, $(r'T{-}Rt')/n{=}(r'{-}R)/r{<}1$, and $(Rt'{-}r'T)/n{<}1{-}r'T/n{<}1$. Thus $s'T{=}St'$ and $(r',s',t') = (R,S,T)$, as $\gcd(s',t'){=}\gcd(S,T){=}1$. $\square$

**Mertens theorem.** $|\sum_{i=2}^k g(i){-}\int_{1.5}^{k+.5} g(x)\,\mathbf{d}x| \le v$, where $v$ is the total variation of $\frac{g'}{8}$. For $g{=}\ln$, $v{<}\frac{1}{12}$, as $g'{=}\frac{1}{x}$ is monotone. So, $\ln(k!) = x\ln\frac{x}{e}|_{1.5}^{k+.5} + \varepsilon$, $\varepsilon{<}\frac{1}{12}$. We estimate $|\mathbb{Z}_n|/|\mathbb{Z}^*_n| = \prod_{p|n}\frac{p}{p-1}$ as $O(\ln k)$, $k \stackrel{\text{df}}{=} \|n\|$ by proving $\sum_{p:\theta(p)\le\ln n}(-\ln(1{-}\frac{1}{p})){\asymp}\sum_{p<k}\frac{1}{p} \asymp \ln(\|k\|)$ ($\asymp$ means "$=O(1)+$"). Let $c(x) \stackrel{\text{df}}{=} \frac{\ln x}{\lceil x\rceil}$ for prime $\lceil x\rceil$, else $c(x) \stackrel{\text{df}}{=} 0$. For $k{=}\sum_i s_i p^i$, $s_i{<}p$ we have $\nu_p(k!){=}\sum_i s_i\nu_p(p^i!){=}\frac{k-\sum_i s_i}{p-1} = \frac{k}{p-1}{-}\frac{t}{\ln p}$, $t{\le}\ln(k{+}1)$. So, $h(k) \stackrel{\text{df}}{=} \int_1^k c(x)\,\mathbf{d}x \asymp \sum_{p\le k}\frac{\ln p}{p-1}{=}\sum_{p\le k}\frac{(\nu_p(k!)\ln p){+}t}{k}{\asymp}\frac{\ln(k!)}{k}{+}\frac{O(\ln k)\pi(k)}{k}{\asymp}\ln k$. By $gh = \int g\,\mathbf{d}h + \int h\,\mathbf{d}g$ for $g(x) \stackrel{\text{df}}{=} \frac{1}{\ln x}$, we get $0 \asymp \int_1^k \frac{c(x)\,\mathbf{d}x}{\ln x} - \int_1^k \frac{h(x)\,\mathbf{d}x}{x(\ln x)^2} \asymp \sum_{p\le k}\frac{1}{p} - \ln\ln k$. $\square$