2.3 The Probability of Flops

Let $n \in \mathbb{N}_3$. Furthermore assume that $u \in \mathbb{N}_2$ is even, $u = r \cdot 2^s$ with odd r and $s \geq 1$. We introduce the sets:

$$\begin{aligned}
A_u^{(0)} &= B_u^{(0)} := \{w \in \mathbb{M}_n \mid w^r = 1\} \quad [\text{case } (\mathrm{E}_{n,u}/\mathrm{I})], \\
A_u^{(t)} &:= \{w \in \mathbb{M}_n \mid w^{r\cdot 2^t} = 1, w^{r\cdot 2^{t-1}} \neq 1\} \quad \text{for } 1 \leq t \leq s, \\
B_u^{(t)} &:= \{w \in A_u^{(t)} \mid w^{r\cdot 2^{t-1}} = -1\} \quad [\text{case } (\mathrm{E}_{n,u}/\mathrm{II})], \\
A_u &:= \bigcup_{t=0}^{s} A_u^{(t)} = \{w \in \mathbb{M}_n \mid w^u = 1\}, \\
B_u &:= \bigcup_{t=0}^{s} B_u^{(t)} \quad [\text{case } (\mathrm{E}_{n,u}) \text{ (I or II)}]. \\
C_0 &:= \{w \in \mathbb{M}_n \mid \operatorname{ord} w \text{ odd}\}, \\
C_1 &:= \{w \in \mathbb{M}_n \mid -1 \in \langle w \rangle\}, \\
C &:= C_0 \cup C_1.
\end{aligned}$$

Remarks

- $A_u^0 \leq A_u \leq \mathbb{M}_n$ are subgroups, as are $A_u^0 \leq C_0 \leq \mathbb{M}_n$.
- $B_u^{(t)} = A_u^{(t)} \cap C$ for $t = 0, \ldots, s$, since a cyclic group $\langle w \rangle$ can contain at most one square root of 1 in addition to 1 itself.
- Hence also $B_u = A_u \cap C$.
- B_u is the exceptional set of "bad" integers with $(\mathrm{E}_{n,u})$ from Section 2.2 that flop with factoring n. The following proposition upper bounds by $\frac{1}{2}$ the probability of hitting an element of this set by pure chance. If we try k random candidate integers the probability of not factoring n is $< 1/2^k$, hence *extremely* small even for moderate sizes of k

Proposition 4 *Let n be odd and not a prime power. Let $u = r \cdot 2^s$ be a multiple of $\lambda(n)$ with odd r. Then*

$$\#B_u \leq \frac{1}{2} \cdot \varphi(n).$$

Proof. By the following lemma C, and a forteriori B_u, is contained in a proper subgroup of $\mathbb{M}_n$. $\diamond$

Lemma 1 (Dixon, AMM 1984) *Let $n \in \mathbb{N}_3$. Assume $\langle C \rangle = \mathbb{M}_n$. Then n is a prime power or even.*

Proof. For this proof let $\lambda(n) = r \cdot 2^s$ with odd r. (Since $n \geq 3$, we have $s \geq 1$. The "old" meanings of r and s don't occur in this proof.) Consider the map

$$h : \mathbb{M}_n \longrightarrow \mathbb{M}_n, \qquad w \mapsto w^{r \cdot 2^{s-1}}.$$

This h is a group homomorphism with $h(\mathbb{M}_n) \subseteq \{v \in \mathbb{M}_n \mid v^2 = 1\}$ (group of square roots of 1 mod$n$). Since the $w \in C_0$ have odd order $h(C_0) \subseteq \{1\}$.

For $w \in C_1$ we have $h(w) \in \langle w \rangle$ and $h(w)^2 = 1$, hence $h(w)$ is one of the two roots of unity $\pm 1 \in \langle w \rangle$.

Together we have $h(C) \subseteq \{\pm 1\}$.

If n is not a prime power (and a forteriori not a prime) there is a decomposition $n = pq$ into coprime factors $p, q \in \mathbb{N}_2$. Since $2^s | \lambda(n) = \mathrm{lcm}(\lambda(p), \lambda(q))$ we may assume $2^s | \lambda(p)$. The chinese remainder theorem provides a $w \in \mathbb{M}_n$ with $w \equiv 1 \pmod{q}$ such that $w \bmod p$ has order 2^s. Then $h(w) \not\equiv 1 \pmod{p}$, a forteriori $h(w) \neq 1$. Since $h(w) \equiv 1 \pmod{q}$ we also have $h(w) \neq -1$—except when $q = 2$.

Therefore if n is not even nor a prime power we have the contradiction $h(\mathbb{M}_n) \not\subseteq \{\pm 1\}$. $\diamond$

This also completes the missing step of Section 2.2: Who knows the private RSA key is able to factor the module n.