# Cryptography, winter term 16/17: Sample solution to assignment 7

Cornelius Brand, Marc Roth

---

**Exercise 7.1 (Uniqueness of inverses and identities)** Let $(G, \cdot)$ be a group.

a) Let $e, e' \in G$ such that for all $g \in G$, $g \cdot e = e \cdot g = e' \cdot g = g \cdot e' = g$. Show that $e = e'$.

b) Let $e$ be as before, and let $g, h, h' \in G$ such that $g \cdot h = h \cdot g = g \cdot h' = h' \cdot g = e$. Show that $h = h'$.

**Solution 7.1 (Uniqueness of inverses and identities)** a) Picking $g = e$ yields $e \cdot e' = e$, and picking $g = e'$ yields $e \cdot e' = e'$. Hence, $e = e'$.

b) $h = eh = (h'g)h = h'(gh) = h'e = h'$.

**Exercise 7.2 (Fast exponentiation in groups)** Let $(G, \cdot)$ be a group. Show that for all positive $n \in \mathbb{N}$, the $n$-th power $g^n$ of $g$ can be computed using $2\log_2 n$ group operations.[1]
**Hint:** Use the identity $g^n = (g^{\lfloor n/2 \rfloor})^2 \cdot g^{n \bmod 2}$.

**Solution 7.2 (Fast exponentiation in groups)** We proceed by induction on $n$. For $n = 1$, obviously $g^1$ can be computed using 0 operations. Assuming that we can compute $g^{n'}$ using $2\log_2 n'$ operations for $n' < n$, observe that from the hint, we need at most $2\log_2 \lfloor n/2 \rfloor + 2 \leq 2\log_2(n/2) + 2 = 2\log_2(n) - 2 + 2 = 2\log_2 n$ operations to compute $g^n$.

**Exercise 7.3 (Divisibility and digit sums)** Prove that a number is divisible by 3 if and only if its digit sum is. Can you see from your proof what other numbers there are between 0 and 10 for which this works? Can you extract a simple criterion for divisibility by 11 from your proof? You may use that reducing modulo $N$ commutes with multiplication and addition, i.e. that $(a + b) \bmod N = (a \bmod N) +_N (b \bmod N)$ and $(a \cdot b) \bmod N = (a \bmod N) \cdot_N (b \bmod N)$, where $+_N$ and $\cdot_N$ denote addition and multiplication modulo $N$.
**Hint:** Consider the base-10 representation of the number to start with, i.e. write $a = \sum_{i=0}^{\infty} a_i 10^i \in \mathbb{Z}$ with $0 \leq a_i < 10$ for all $i$.

[1] To be more precise on the model of computation, we allow intermediate results to be reused, i.e. once you have computed some element $g$ using $T$ operations, $g^2$ can be computed in a single operation.

**Solution 7.3 (Divisibility and digit sums)** We can write $a = \sum_{i=0}^{\infty} a_i 10^i \in \mathbb{Z}$ with $0 \leq a_i < 10$ for all $i$. Modulo 3, this gives (using the hint)

$$
\begin{aligned}
a \bmod 3 = & \\
& \left(\sum_{i=0}^{\infty} a_i 10^i\right) \bmod 3 = \sum_{i=0}^{\infty} (a_i \bmod 3)(10 \bmod 3)^i = \\
& = \sum_{i=0}^{\infty} (a_i \bmod 3)(1^i \bmod 3) = \sum_{i=0}^{\infty} \left(a_i \cdot 1^i \bmod 3\right) = \\
& \sum_{i=0}^{\infty} (a_i \bmod 3) = \left(\sum_{i=0}^{\infty} a_i\right) \bmod 3
\end{aligned}
$$

The only other number between 0 and 10 for which this proof goes through (i.e. that satisfies $10 = 1 \bmod N$) is 9. Divisibility by 11 is likewise characterized by divisibility by 11 of the *alternating* digit sum, defined by $\sum_{i=0}^{\infty} (-1)^i a_i$ or $\sum_{i=0}^{\infty} (-1)^{i+1} a_i$, which doesn't influence divisibility.

**Exercise 7.4 (Chinese Remaindering)** Using the Chinese Remainder Theorem, compute by hand $46^{51} \bmod 55$ and $16^{232311} \bmod 68$.

**Solution 7.4 (Chinese Remaindering)** Writing $55 = 5 \cdot 11$, we find that $x = 46^{51} = 1 \bmod 5$ and $x = 46^{51} = (2^{10})^5 \cdot 2 = 2 \cdot 1^5 = 2 \bmod 11$ and therefore $46^{51} = 46 \bmod 55$.

Similarly, $68 = 4 \cdot 17$, and $x = 16^{232311} = -1 \bmod 17$, $x = 0 \bmod 4$, making $16^{232311} \bmod 68 = 16 \bmod 68$