Answers to Homework 1

Leonhard Horstmeyer (Leo Marlo#1048)

February 8, 2023

Question 1

Odd Squares: I think I can actually prove this. So we know that

$$(a+b) \bmod N \equiv a \bmod N + b \bmod N \tag{1}$$

from modular arithmetics. In other words (writing out the definition of equivalence $\equiv$):

$$(a+b) \bmod N = (a \bmod N + b \bmod N) \bmod N \tag{2}$$

So let x be some odd number, that is for any x there exists a natural number $y \in \mathbb{N}$ such that $x = 2y+1$.
We prove by induction. For $x = 1$ the statement is obviously true, since $1^2 \bmod 8 = 1$. Suppose now that $x^2 \bmod 8 = c$, where $c = 1$ in our case. Then consider the next odd number $x+2$:

$$\begin{aligned}
(x+2)^2 \bmod 8 &= \left(x^2 + 4x + 4\right) \bmod 8 \\
&= \left(x^2 \bmod 8 + (4x) \bmod 8 + 4 \bmod 8\right) \bmod 8 \\
&= (c + (4x) \bmod 8 + 4) \bmod 8 \\
&= (c + (8y+4) \bmod 8 + 4) \bmod 8 \\
&= (c + ((8y) \bmod 8 + 4 \bmod 8) \bmod 8 + 4) \bmod 8 \\
&= (c + 4 \bmod 8 + 4) \bmod 8 \\
&= (c+8) \bmod 8 = c = 1
\end{aligned} \tag{3}$$

Even squares: For even squares the situation is the same, except that the result is always 4, i.e. $x^2 \bmod 8 = 4$. For $x = 2$ the result is obviously true. Let's now assume it is true for some even x, then for $x+2$ we go through the same calculation as above, except that we take $c = 4$.

Question 3

1. $\mathcal{O}(n)$ means that as we take the limit $n \to \infty$ the thing divided by n converges to a non-zero and non-infinite number.
2. $\mathcal{O}(1)$ means that as we take the limit $n \to \infty$ the thing converges to a non-zero and non-infinite number.
3. $\mathcal{O}(\log n)$ means that as we take the limit $n \to \infty$ the thing divided by $\log n$ converges to a non-zero and non-infinite number.

Here $\mathcal{O}(n)$ is the worst behaved, then comes $\mathcal{O}(\log n)$. The best is $\mathcal{O}(1)$.