1. série domácích úloh z Algebry

Řešení odevzdávejte do úterý **5. března 24:00.**

Pokud někde v řešení použijete nějakou větu z přednášky (např. Eulerovu nebo ČZV), nezapomeňte to explicitně uvést a ověřit předpoklady!

Úloha 1 (2 body)**.** Určete inverzní prvek k 2024 v tělese $\mathbb{Z}_{4001}$.

Úloha 2 (3 body)**.** Aby Bedřich dobře utajil svou komunikaci, rozhodl se použít protokol RSA; jako veřejný klíč zvolil čísla $N = 187$ a $e = 23$. Amálie vzala zprávu $x \in \{1, \ldots, 186\}$, zašifrovala ji dle protokolu a následně odeslala Bedřichovi číslo $y = 5$. Jakou zprávu x Amálie zakódovala? *Tento typ úlohy nebude na cvičení, vyřešte ho přímo podle popisu RSA z přednášky nebo skript.*

Úloha 3 (2 body)**.** Určete zbytek $17^{19^{777}}$ po dělení 70.

Úloha 4 (3 body)**.** Na školní výlet jeli studenti autobusy o 65 místech, přičemž nastupovali tak, že vždy naplnili celý autobus, ten odjel, pak nastupovali do dalšího atd. V posledním autobuse jich pak bylo už jen deset. Později pak jeli čtyřmístnou lanovkou, na kterou nasedali obdobně, přičemž na poslední sedačce pak jel jen jeden. Kolik studentů se zúčastnilo výletu, jestliže jich bylo méně než 500? Nalezněte všechny možnosti.