4. obligatoriske hjemmeopgave i ElmTal

Prøven består af 6 spørgsmål, der alle skal besvares. Besvarelsen afleveres senest tirsdag den 26. januar ved øvelserne.

1. Min offentlige RSA-nøgle er $(33, 7)$. Restklasserne $0, \dots, 32$ modulo 33 fortolkes som de 29 danske bogstaver efterfulgt af de 4 specialtegn: '.', ',', '!', '?'. En student sender mig h-teksten ÅPFLØE. Hvad var klarteksten?

2. Lad $p > 2$ være et primtal. Vis, at hvis $[a]_p$ frembringer $(\mathbb{Z}/p)^*$, så er $\left(\frac{a}{p}\right) = -1$. Vis, at hvis p er et Fermat-primtal, så gælder også det omvendte. Vis, at hvis p ikke er et Fermat-primtal, så findes et tal a således, at $\left(\frac{a}{p}\right) = -1$ og $[a]_p$ er *ikke* en frembringer for $(\mathbb{Z}/p)^*$.

3. Tabellen herunder er uddrag af en tabel med søjler svarende til tallene $n = 2, 3, 4, \dots, 22$. Under n i første rækkke står i anden række primopløsningen af $M_n = 2^n - 1$, og i tredie række de primtal p, for hvilke restklassen $[2]_p$ har orden n i $(\mathbb{Z}/p)^*$. Forklar, hvordan man kan få tredie række ud fra tabellens anden række.
Kompleter tabellen, så den indeholder resultaterne for alle $n = 2, 3, 4, \dots, 21$. Du må gerne overspringe de n, for hvilke M_n er et Mersenne-primtal. Det er nok, at du anfører tabellens tredie række.

2	3	4	5	6	......	11	......	21
3	7	$3 \cdot 5$	31	$3^2 \cdot 7$	......	$23 \cdot 89$	......	
3	7	5	31		......	23, 89	......	337

[Vink: Du behøver i hvert fald ikke at beregne potenser af 2 større end 2^{10}. Ultimativt kan du faktorisere $2^n - 1$ ved at bruge, at $2^n - 1 = \prod_{d \mid n} \Phi_d(2)$, men du kan såmænd nøjes med at bruge, at hvis $n = qd$ er sammensat, så er $2^d - 1$ divisor i $2^{qd} - 1$; ja, faktisk kan du nøjes med at udnytte, at $2^{2d} - 1 = (2^d - 1)(2^d + 1)$.]
Bestem det mindste primtal p, for hvilket der gælder, at $\left(\frac{2}{p}\right) = -1$ og $[2]_p$'s orden er mindre end $p - 1$.

4. Lad $\mathcal{E}_n$ betegne gruppen af de permutationer af $\mathbb{Z}/n$, der er af formen $x \mapsto x^e$. Antag, at $n = 17 \cdot 19$. Bestem gruppen $\mathcal{E}_n$. Vis, at den maksimale orden af en permutation i $\mathcal{E}_n$ er 12. Hvilken orden har permutationen $x \mapsto x^5$? Bryd koden bestemt ved RSA-nøglen $(323, 5)$ (dvs bestem d svarende til $e = 5$).

5. Vis følgende uligheder (den første kun for $n > 1$):

$$2 \leqslant \tau(n) < 2\sqrt{n}, \qquad n \leqslant \sigma(n) < 2n\sqrt{n},$$
$$\sqrt{n/2} \leqslant \varphi(n) \leqslant n, \qquad n^2/2 < \varphi(n)\sigma(n) \leqslant n^2.$$

[Du må bruge vinkene, der står i noterne ved den tilsvarende opgave!]

6. Vis, at udtrykket i formlen (8.9.1) for $\alpha_p(n)$ er positivt for alle n, også når $p \geqslant 2$ ikke er et primtal.