Tentamen i MMG100 Elementär talteori 2019 – 09 – 28 kl 8.30 – 12.30

Examinator: Johan Berglind
Telefonvakt: Carl-Joar Karlsson, ankn 5325
Hjälpmedel: Inga

För godkänt krävs 12 poäng, för väl godkänt 18 poäng.

Motivera alla svar väl.

1. Bestäm alla primtal *p* sådana att $2^p + 1$ är delbart med *p*. **(3p)**

2. Bestäm alla udda primtal *p* sådana att kongruensen
   $x^4 + 1 \equiv 0 \ \ (mod\ p)$ har minst en lösning. **(3p)**

3. Om både *p* och $p + 2$ är primtal kallas de ***primtalstvillingar***.
   Visa att det finns oändligt många primtal som inte är primtalstvillingar.
   Det är tillåtet att använda Dirichlet's sats: följden
   $an + b, \ n = 1, 2, 3, \ldots$, där *a* och *b* är relativt prima, innehåller
   oändligt många primtal. **(3p)**

4. Avgör om det finns ett positivt heltal *n* sådant att
   talen $n, n + 1, n + 2, n + 3, \ldots, n + 2019$ alla är sammansatta. **(2p)**

5. I ett RSA-krypto är $n = 2627 = 37 \cdot 71$. Exponenten *e* är okänd,
   men vi vet att *e* ***inte*** är ett primtal, samt att $e < 200$.
   Vi söker *d*, inversen till *e*, för att kunna dekryptera. Hur många
   möjliga värden för *e* finns det? Bestäm *d* för ett av dem. **(3p)**

6. Antag att $2n$ punkter ligger utspridda på enhetscirkeln (*n* är ett positivt heltal).
   Hälften av punkterna är färgade blå, den andra hälften röda. En ***promenad*** går till så att vi rör oss ett varv moturs längs enhetscirkeln och räknar röda och blå punkter. En ***behaglig promenad*** är en promenad sådan att vi i varje givet ögonblick har passerat minst lika många blå som röda punkter.
   Visa med induktion att det alltid existerar en startpunkt (ej en färgad punkt) från vilken vi kan ta en behaglig promenad. **(3p)**

7. Bestäm alla primtal *p* sådana att $2^{p-2} + 3^{p-2} + 6^{p-2} \equiv 1 \ (mod\ p)$ **(3p)**

8. Låt *p* vara ett udda primtal och $S_n = 1^n + 2^n + 3^n + \cdots + (p-1)^n$
   där *n* är ett positivt heltal.
   Visa att $S_n \equiv 0 \ (mod\ p)$ eller $S_n \equiv -1 \ (mod\ p)$
   För vilka *n* gäller den första kongruensen? **(5p)**