53. **Die Schlacht von Hastings** (14.10.1066):
Harolds Mannen standen dicht gedrängt in 13 gleich großen Quadraten aufgestellt, und wehe dem Normannen, der es wagte, in eine solche Phalanx einbrechen zu wollen... Als aber Harold selbst auf dem Schlachtfeld erschien, formten die Sachsen ein einziges gewaltiges Quadrat mit ihrem König an der Spitze und stürmten mit den Schlachtrufen "Ut!", "Olicrosse!", "Godemite!" vorwärts... (vgl. *"Carmen de Hastingae Proelio"* von Guy, Bischof von Amiens

Wie groß soll die Armee Harolds II. gewesen sein?

54. Es sei $d < 0$ und $p \in \mathbb{Z}$ eine Primzahl.

(a) Zeige: Ist die Gleichung $N(\alpha) = p$ für $\alpha \in \mathbb{Z}[\sqrt{d}]$ unlösbar, dann ist p zu einem in $\mathbb{Z}[\sqrt{d}]$ irreduziblen Element π assoziiert.

(b) Zeige: Ist die Gleichung $N(\alpha) = p$ für $\alpha \in \mathbb{Z}[\sqrt{d}]$ lösbar, dann ist α in $\mathbb{Z}[\sqrt{d}]$ irreduzibel.

(c) Zeige: Falls $\pi \in \mathbb{Z}[\sqrt{d}]$ prim ist, dann ist π entweder eine Primzahl in $\mathbb{Z}$ der Form (a), oder aber $N(\pi) = p$ ist eine Primzahl in $\mathbb{Z}$ (und wir sind im Fall (b)).

(d) Was geschieht im Fall $d > 0$?

55. Es sei $\mathcal{O}$ der Ring der ganzen algebraischen Zahlen.
Zeige: $\mathbb{Q} \cap \mathcal{O} = \mathbb{Z}$ (mit anderen Worten: "$\mathbb{Z}$ ist *ganzabgeschlossen*").

56. Zeige: Der Ring $\mathcal{O}[\sqrt{-7}] := \mathcal{O} \cap \mathbb{Q}[\sqrt{-7}] = \mathbb{Z}\left[\frac{-1+\sqrt{-7}}{2}\right]$ ist ein euklidischer Ring.
(Verwende als Norm $N(x + \alpha y) = (x + \alpha y)(x + \overline{\alpha} y)$, $\alpha = \frac{-1+\sqrt{-7}}{2}$.)
Wie verträgt sich das mit den Zerlegungen: $8 = (1 + \sqrt{-7})(1 - \sqrt{-7}) = 2^3$?

57. Zeige: Es gibt unendlich viele Primzahlen der Form $4k + 3$, $k \in \mathbb{N}$.

58. Zeige: Falls $p \equiv 1(4)$, $p \in \mathcal{P}$, dann gilt $X^2 + 1 | X^{p-1} - 1$.

59. Zeige: Falls $p \equiv 1(4)$, $p \in \mathcal{P}$, dann ist die Kongruenz $x^2 \equiv -1(p)$ lösbar.

60. Beweise die Multiplikativität des Legendre-Symbols:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

61. (a) Beweise: $(X^{p-1} - \overline{1}) = (X - \overline{1})(X - \overline{2}) \cdot \ldots \cdot (X - \overline{p-1})$.

(b) Was ergibt sich für $X = 0$?