Aufgaben

Aufgabe 1.

a. Finden Sie die Fundamentallösung der Gleichung $x^2 - 119y^2 = 1$.

b. Hat die Gleichung $x^2 - 119y^2 = -1$ ganzzahlige Lösungen?

Aufgabe 2. Die Schlacht von Hastings. (14.10.1066)
Harolds Mannen standen nach alter Gewohnheit dichtgedrängt in 37 gleichgroßen Quadraten aufgestellt, und wehe dem Normannen, der es wagte, in eine solche Phalanx eingrechen 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...
Wie groß war Harolds Armee mindenstens?

Aufgabe 3. Ein Pythagoräisches Dreieck ist ein rechtwinkliges Dreieck, dessen Seitenlängen natürliche Zahlen sind. Finden Sie alle Pythagoräischen Dreiecke, bei denen die Differenz der Kathetenlängen eins beträgt.

Aufgabe 4. Diese Aufgabe benutzt die Notation von §7 der Vorlesung (RSA-Verfahren).

a. Falls $p < q < 2p$ und $3d < n^{\frac{1}{4}}$ ist, dann gilt für $k = \frac{ed-1}{\varphi(n)}$:
$$\left|\frac{e}{n} - \frac{k}{d}\right| \leq \frac{1}{3d^2}.$$

b. Geben Sie einen (schnellen) Algorithmus an, welcher im Fall $p < q < 2p$ und $3d < n^{\frac{1}{4}}$ aus dem öffentlichen Schlüssel (n, e) den privaten Schlüssel (n, d) berechnet.

Die Blätter sollen bis Donnerstag, den 29.01. um 14.15 Uhr in die dafür vorgesehenen Einwurfkästen im Foyer des Mathematischen Instituts abgegeben werden.