**Number theory exercises WS 2019, TU Graz**

**Sheet 5, solutions (on paper) to be handed in on 7th January 2020**

**5-1.** The four squares theorem can be generalised: For every $k$ let $g(k)$ be the least integer such that every positive integer $n$ is a sum of $g(k)$ $k$th powers. (Hence $g(2) = 4$.) Hilbert proved that $g(k)$ is finite, for all positive $k$. In this exercise you shall give an upper bound on $g(4)$ and $g(6)$.

(a) Use an identity of Liouville (below) to prove that every integer is a sum of at most 53 fourth powers.

$$\begin{aligned}&6(a^2+b^2+c^2+d^2)^2 =\\ &+(a+b)^4+(a-b)^4+(a+c)^4+(a-c)^4+(a+d)^4+(a-d)^4\\ &+(b+c)^4+(b-c)^4+(b+d)^4+(b-d)^4+(c+d)^4+(c-d)^4\end{aligned}$$

(b) Let

$$\begin{aligned}\textstyle\sum_1 =\ & \textstyle\sum_{a\cdots d}^{16}[a\pm b\pm c]^6\\ =\ & +(a+b+c)^6+(-a+b+c)^6+(a-b+c)^6+(a+b-c)^6\\ & +(a+b+d)^6+(-a+b+d)^6+(a-b+d)^6+(a+b-d)^6\\ & +(a+c+d)^6+(-a+c+d)^6+(a-c+d)^6+(a+c-d)^6\\ & +(b+c+d)^6+(-b+c+d)^6+(b-c+d)^6+(b+c-d)^6.\end{aligned}$$

$$\begin{aligned}\textstyle\sum_2 =\ & 2\textstyle\sum_{a\cdots d}^{12}[a\pm b]^6 =\\ & +2(a+b)^6+2(a-b)^6+2(a+c)^6+2(a-c)^6+2(a+d)^6+2(a-d)^6\\ & +2(b+c)^6+2(b-c)^6+2(b+d)^6+2(b-d)^6+2(c+d)^6+2(c-d)^6.\end{aligned}$$

$$\textstyle\sum_3 = 36\sum_{a\cdots d}^{4}[a]^6 = 36a^6+36b^6+36c^6+36d^6.$$

Verify (for example using a Computer algebra package, or by observing which terms cancel) that

$$\sum_1+\sum_2+\sum_3 = 60(a^2+b^2+c^2+d^2)^3.$$

From this prove that every integer $60n+i$ is a sum of at most ... sixth powers, i.e. prove that $g(6)$ is finite and give an upper bound on it.
Also give a lower bound on $g(6)$, by studying “small” integers which need many powers $1^6$ and $2^6$.

**5-2.** Prove that 1 has infinitely many different representations as the sum of three cubes (including negative cubes). Hint: study

$$(9x^4)^3+(3x-9x^4)^3+(1-9x^3)^3 = 1.$$

From this (or otherwise) prove that

$$(9m^4)^3+(3mn^3-9m^4)^3+(n^4-9m^3n)^3 = n^{12}.$$

From this prove that the number $r_{3,3}(N)$ of representations of $N = n^{12}$ as a sum of 3 positive cubes is $r_{3,3}(N) \geq 9^{-1/3}N^{1/12}$.

Look up “Conjecture K” of Hardy and Littlewood and observe that the example above gives a counter example to that conjecture.

**5-3.** Prove the following Theorem, by verifying (and giving some more details) to the outline below.
Theorem: A positive-definite binary quadratic form of discriminant 1 represents an odd prime

$p$ if and only if $p \equiv 1 \bmod 4$. (This shall use some of the theory of binary quadratic forms, relating it to $x^2+y^2$, but do *not* use that primes $p \equiv 1 \bmod 4$ can be written in this form!)

Sketch proof: If $p \equiv 1 \bmod 4$, then $m^2 \equiv -1 \bmod p$ has a solution. Let $m^2 = -1 + np$. (Can we choose $m$ to be even?) Define the following quadratic form:

$$f(x,y) = px^2 + 2\frac{m}{2}xy + ny^2.$$

This form has discriminant 1, is positive definite and respresents $p$ (choose $(x,y) = (1,0)$). Every form which is equivalent to $f$ represents the same integers. Now, for discriminant $d = 1$, there is only one equivalence class. Hence $f$ is equivalent to $f_2(x,y) = x^2 + y^2$. Hence $f_2$ respresents $p$. Conversely, for $p \equiv 3 \bmod 4$: these are not represented by $f_2$, hence not represented by any other positive-definite binary quadratic form of discriminant 1.

**5-4.** (not to be handed in, unless you make an interesting observation) Think about an identity of type $(x_1^2 + x_2^2 + x_3^2)(y_1^2 + y_2^2 + y_3^2) = (z_1^2 + z_2^2 + z_3^2)$.

Thinking about it, quaternions were discovered! For some history, see:
http://www.maths.tcd.ie/pub/HistMath/People/Hamilton/Letters/BroomeBridge.html

Other identities: http://sites.google.com/site/tpiezas/004

Hand in solutions to problems 5.1-5.3

Deadline for crosses are: Tuesday 9.55am.

`https://www.math.tugraz.at/~elsholtz/WWW/lectures/ws19/numbertheory/vorlesung.html`

Possibly the problem sheet will be extended a bit. You have about 4 weeks of time...

Happy Christmas!