A little bit of number theory

In the following few pages, several arithmetical theorems are stated. They are meant as a sample. Some are old, some are new. The point is that one now knows, for the reasons stated below, that there are infinitely many theorems of the same types. Theorems 1, 2 and 3 follow, at the cost of some simple calculations, from 16 of Jacquet-Langlands. Theorem 1 seems to have been known to Liouville (Dickson, History, vol. 3, ch. X). Theorem 4 is already implicit in Hecke (p. 901 of his *Mathematische Werke*). Theorem 5 is due to Deuring. Theorem 6 is a consequence of Theorems 3 and 5. Theorem 7 follows from Vélu's results, Comptes Rendus, v. 273, p. 73 (N.B. he assumes the Weil conjecture relating elliptic curves and modular varieties), and 16 of J.-L. Theorems 1, 2, and 3 are typical consequences of the general theorems stated there. That chapter and the results of the representation volume of the Antwerp lectures imply that a theorem like Theorems 4, 6 and 7 is valid for any elliptic curve satisfying the Weil conjecture, provided that the associated ℓ-adic representation of $\mathfrak{G}(\overline{\mathbb{Q}}_p/Q_p)$ is for at least one $p(\neq \ell)$ not the direct sum of two one-dimensional representations. ℓ is of course arbitrary.

I have been unable to convince myself that the theorems are *trivial*. As I said in a letter to Weil almost six years ago, one can hope that the theory of automorphic forms on reductive groups will eventually lead to general theorems of the same sort (cf. the last paragraph of "*Problems in the theory of automorphic forms*").

The theorems are all of the following form. For each prime p not in a certain finite set two integers A_p and B_p are defined. The conclusion is that $A_p = B_p$ for all these p.

Theorem 1. (a) *If* $p \equiv 3 (\mathrm{mod} 4)$ *then* $A_p = 0$. *If* $p \equiv 1 (\mathrm{mod} 4)$, *let* $p = x^2 + y^2$ *with* (x, y) *congruent to* $(1, 0)$ *or to* $(-1, 2)$ *modulo* 4. *Then* $A_p = 2x$.

(b) If $p \equiv 3 (\mathrm{mod} 4)$ *then* B_p *is the number of solutions of*

$$\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = p$$

with $\alpha \equiv 1 (\mathrm{mod} 4)$, (β, γ, δ) *congruent modulo* 4 *to one of* $(0, 1, 1)$, $(2, 3, 3)$, $(0, 3, 3)$, $(2, 1, 1)$ *minus the number with* $\alpha \equiv 1 (\mathrm{mod} 4)$ *and* (β, γ, δ) *congruent to one of* $(0, 3, 1)$, $(2, 1, 3)$, $(0, 1, 3)$, $(2, 3, 1)$ *modulo* 4. *If* $p \equiv 1 (\mathrm{mod} 4)$ *then* B_p *is equal to the number of solutions of* *the same equation with* $\alpha \equiv 1(\mathrm{mod}4)$ *and* (β, γ, δ) *congruent to one of* $(0,0,0)$, $(2,0,0)$, $(0,2,2)$, $(2,2,2)$ *minus the number with* $\alpha \equiv 1(\mathrm{mod}4)$, (β, γ, δ) *congruent to one of* $(2,2,0)$, $(0,2,0)$, $(2,0,2)$, $(0,0,2)$.

Theorem 2 *(a) If* $p \equiv 3(\mathrm{mod}4)$ *then* $A_p = 0$. *If* $p \equiv 1(\mathrm{mod}4)$ *write* $p = x^2 + y^2$ *as in the preceding theorem and set* $A_p = 2(x^3 - 3xy^2)$.

(b) If $p \equiv (\mathrm{mod}4)$ *set*

$$B_p = \sum \{\alpha^2 + \beta^2 - \gamma^2 - \delta^2\} - \sum \{\alpha^2 + \beta^2 - \gamma^2 - \delta^2\}$$

The first sum is over 4*-tuples such that* $\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = p$, $\alpha \equiv 1(\mathrm{mod}4)$, *and* (β, γ, δ) *is congruent modulo* 4 *to one of* $(0,1,1)$, $(2,3,3)$, $(0,3,3)$, $(2,1,1)$. *The second sum is similar but now* (β, γ, δ) *is congruent to one of* $(0,3,1)$, $(2,1,3)$, $(0,1,3)$, $(2,3,1)$.

But if $p \equiv (\mathrm{mod}4)$ *set*

$$B_p = \sum \{\alpha^2 + \beta^2 - \gamma^2 - \delta^2\} - \sum \{\alpha^2 + \beta^2 - \gamma^2 - \delta^2\}$$

The two sums are defined similarly. Again $\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = p$ *and* $\alpha \equiv 1(\mathrm{mod}4)$, *but in the first sum* (β, γ, δ) *is congruent modulo* 4 *to one of* $(0,0,0)$, $(2,0,0)$, $(0,2,2)$, $(2,2,2)$ *and in the second to one of* $(2,2,0)$, $(0,2,0)$, $(2,0,2)$, $(0,0,2)$.

Theorem 3. *(a) Let* χ *be the unique quadratic character modulo 11. If* $p \neq 11$

$$A_p = \frac{1}{2} \sum_{x^2+xy+3y^2=p} \chi(x + \frac{y}{2})(x + \frac{y}{2}).$$

(b) Let ϵ *be the function on* $\mathbb{F}_{11} \times \mathbb{F}_{11} - \{(0,0)\}$ *given by the table below.*

$b \setminus a$	0	1	2	3	4	5	6	7	8	9	10
0		1	1	1	1	1	1	1	1	1	1
1	-1	$-i$	1	$-i$	$-i$	-1	-1	i	i	1	i
2	-1	-1	$-i$	i	1	i	$-i$	1	$-i$	i	-1
3	-1	$-i$	i	$-i$	-1	1	1	-1	i	$-i$	i
4	-1	$-i$	-1	1	$-i$	$-i$	i	i	1	-1	i
5	-1	1	i	-1	$-i$	$-i$	i	i	-1	$-i$	1
6	-1	1	$-i$	-1	i	i	$-i$	$-i$	-1	i	1
7	-1	i	-1	1	i	i	$-i$	$-i$	1	-1	$-i$
8	-1	i	$-i$	i	-1	1	1	-1	$-i$	i	$-i$
9	-1	-1	i	$-i$	1	$-i$	i	1	i	$-i$	-1
10	-1	i	1	i	i	-1	-1	$-i$	$-i$	1	$-i$

Then B_p is

$$B_p = \frac{1}{6} \sum \epsilon(x + \frac{y}{2}, u + \frac{v}{2})$$

In the sum

$$x^2 + xy + 3y^2 + u^2 + uv + 3v^2 = 4p$$

and $x \equiv v (\mathrm{mod} 2)$, $y \equiv 0 (\mathrm{mod} 2)$, $y + u \equiv 0 (\mathrm{mod} 2)$.

Theorem 4. *(a) If $p \neq 11$ let $p - A_p, p - A'_p, p - A''_p$ be respectively the number of points on the following affine curves modulo p.*

$$\begin{aligned} E: &\quad y^2 + y = x^3 - x^2; \\ E': &\quad y^2 + y = x^3 - x^2 - 10x - 20; \\ E'': &\quad y^2 + y = x^3 - x^2 - 7820x - 263580. \end{aligned}$$

Then $A_p = A'_p = A''_p$.

(b) If $p \neq 11, B_p$ is one-quarter the number of representations of p by

$$x^2 + xy + 3y^2 + u^2 + uv + 3v^2$$

minus $\frac{1}{4}$ the number of representations of p by

$$2(x^2 + y^2 + u^2 + v^2) + 2xu + xv + yu - 2yv.$$

Theorem $4'$. *(a) If $p \neq 11$ let $p - A_p, p - A'_p, p - A''_p$ be respectively the number of points on the following affine curves modulo p.*

$$F : y^2 + y = x^3 - x^2 - 40x - 221 \qquad (7);$$

$$F' : y^2 + y = x^3 - x^2 - 1250x + 31239;$$

$$F'' : y^2 + y = x^3 - x^2 - 946260x + 354609639.$$

Then $A_p = A'_p = A''_p$.

(b) B_p is the B_p of the previous theorem multiplied by $\chi(p)$.

Theorem 5. *(a) If $p \neq 11$ let $p - A_p, p - A'_p$ be respectively the number of points on the following affine curves modulo p.*

$$D : y^2 + y = x^3 - x^2 - 7x + 10;$$

$$D' : y^2 + y = x^3 - x^2 - 887x - 10143.$$

Then $A_p = A'_p$.

(b) If $p \neq 11$

$$B_p = \frac{1}{2} \sum_{x^2+xy+3y^2=p} \chi(x + \frac{y}{2})(x + \frac{y}{2}).$$

Theorem 6. *(a) A_p is defined as in Theorem 5.*

(b) B_p is defined as in Theorem 3.

Theorem 7. *(a) If $p \neq 11$ let $p - A_p, p - A'_p$ be respectively the number of points on the following affine curves modulo p.*

$$E : y^2 + xy = x^3 + x^2 - 2x - 7;$$

$$F : y^2 + xy = x^3 + x^2 - 3632x + 82757.$$

Then $A_p = A'_p$.

(b) B_p, $p \neq 11$ is equal to one-quarter the number of representations of p by

$$x^2 + xy + 3y^2 + u^2 + uv + 3v^2$$

with $x + \frac{y}{2}$, $u + \frac{v}{2}$, $(x + \frac{y}{2}) - (u + \frac{v}{2})$, *or* $(x + \frac{y}{2}) + (u + \frac{v}{2})$ *congruent to* 0 *modulo 11 minus* $\frac{1}{8}$ *the number of representations not satisfying this condition.*

Theorem 7'. *(a) If* $p \neq 11$ *let* $p - A_p, p - A'_p$ *be respectively the number of points on the following affine curves modulo* p*.*

$$E' : y^2 + xy + y = x^3 + x^2 - 305x + 7888;$$

$$F' : y^2 + xy + y = x^3 + x^2 - 30x - 76.$$

Then $A_p = A'_p$*.*

(b) Take the B_p *of the previous lemma and multiply by* $\chi(p)$*.*