

Algebraic Number Theory

Robert F. Coleman

Lecture 21

Dwork's Lemma

Lemma. Suppose $F(X) \in 1 + X\mathbf{Q}_p[[X]]$. Then $F(X) \in \mathbf{Z}_p[[X]]$ if and only if $F(X^p)/F(X)^p \equiv 1 \pmod{p}$.

Proof.

Examples. Artin-Hasse

$$\exp\left(\sum \frac{x^{p^i}}{p^i}\right)$$

Let

$$F(X, Y) = (1 + Y)^X (1 + Y^p)^{\frac{X^p - X}{p}} \cdots (1 + Y^{p^n})^{\frac{X^{p^n} - X^{p^{n-1}}}{p^n}} \cdots$$

Now fix ζ be a primitive p -th root of 1 and set

$$\Theta(T) = F(T, \zeta - 1).$$

Proposition. Suppose $|k| = q = p^s$. Then $\Theta(T) \in R_{1,1/(p-1)}$ and

$$\Theta(\tau(a))\Theta(\tau(a)^p) \cdots \Theta(\tau(a)^{p^{s-1}}) = \zeta^{\mathrm{Tr}_{\mathbf{F}_p}^k(a)}.$$

Proof. We can write

$$F(X, Y) = \sum_{n \geq 0} (X^n \sum_{m \geq n} a_{m,n} Y^m)$$

Suppose $t^{q-1} = 1$. Then

$$(1 + Y)^{1+t+\dots+t^{p^{s-1}}} = F(t, Y)F(t^p, Y) \cdots F(t^{p^{s-1}}, Y)$$