PRIME TIME SEMINAR
VENUE: LH-1, DEPARTMENT OF MATHEMATICS, IISC BENGALURU

IRISH DEBBARMA, MASTERS STUDENT

1 NOTATION

Let $\mathbb{F}_q$ be a finite field with $q = p^r$ elements where p a prime number and $r \in \mathbb{Z}_{>0}$.

2 SOLUTIONS TO $x^n = u$

Let $N(u)$ be the number of solutions in $\mathbb{F}_q$ to the equation $x^n = u$.
Clearly, if $u = 0$ then $x = 0$. So, suppose $u \neq 0$. Since $\mathbb{F}_q^\times$ is a cyclic group, with say generator w, $\mathbb{F}_q \ni u \neq 0$ can be written as $u = w^k$. If x is a solution to $x^n = u$, then x is non-zero and thus can be written as $x = w^\ell$. Consequently, x is a solution if and only if $w^{\ell n} = w^k \Leftrightarrow w^{\ell n - k} = 1 \Leftrightarrow \ell n \equiv k \pmod{q-1}$ if and only if $\gcd(n, q-1) \mid k$. To summarise,

$$N(u) = \begin{cases} 1 & , u = 0 \\ d := \gcd(n, q-1) & , u \neq 0 \end{cases}$$

Lemma 1. *The solution set of $x^n = u$ is in bijection with the solution set of $x^d = u$ with $u \neq 0$.*

Remark 2. *I just need that the size of the two solution sets is the same.*

Proof. Let $u = w^k$. If $x \in \mathbb{F}_q$ such that $x^n = u$, then $x^{dd'} = u \Rightarrow (x^{d'})^d = u$ and thus $x^{d'}$ is a solution to $x^d = u$. Conversely, suppose $x^d = u$ for some $x \in \mathbb{F}_q$. As $d = \gcd(n, q-1)$, there are integers $s, t \in \mathbb{Z}$ such that $ns + t(q-1) = d$. Therefore,

$$x^d = x^{ns + t(q-1)} = (x^s)^n \cdot 1 = (x^s)^n = u$$

Hence, we have a bijection between the two solution sets. This completes the proof. □

This allows us to assume without loss of generality that $n \mid q-1$.

Lemma 3. *The number of solutions to the equation $x^n = u$ in $\mathbb{F}_q$, denoted by $N(u)$ is given by $\sum_{\chi^n = \mathbf{1}} \chi(u)$.*

Date: October 2023.

3 Solutions to $a_0x_0^{n_0} + a_2x_2^{n_2} + \cdots + a_rx_r^{n_r} = 0$

This section follows Weil's paper [Wei49]. Let $a_0, a_1, \ldots, a_r \in \mathbb{F}_q$, and $n_0, n_1, \ldots, n_r \in \mathbb{Z}$. We can assume all the n_i's are positive (only small modifications is required for negative exponents). We want to find the number of solutions N of the equation

$$a_0x_0^{n_0} + a_1x_1^{n_1} + \cdots + a_rx_r^{n_r} = 0 \tag{1}$$

in $\mathbb{F}_q$. For each i, let $d_i = \gcd(n_i, q-1)$ and $N_i(u)$ be the number of solutions of $x^{n_i} = u$. If we put $L(u) = \sum_{i=0}^{r} a_iu_i$, we find that

$$N = \sum_{L(u)=0} N_0(u_0)N_1(u_1)\cdots N_r(u_r) \tag{2}$$

where the sum is over all tuples $(u_0, \ldots, u_r)$ such that $L(u) = 0$.

Definition 4. *Fix the map $\phi : \overline{\mathbb{F}}_q^\times \to \mathbb{C}^\times$. Let $\alpha \in \mathbb{Q}/\mathbb{Z}$ and $n \in \mathbb{Z}_{>0}$ such that $(q^n - 1)\alpha \equiv 0 \pmod 1$. Define $\chi_{\alpha,n} : \mathbb{F}_q^\times \to \mathbb{C}^\times$ by*

$$\chi_{\alpha,n}(x) = \phi(x)^{(q^n-1)\alpha}$$

We can extend this to $\mathbb{F}_q$ by defining at 0. We do that by

$$\chi_{\alpha,n}(0) = \begin{cases} 0 & ,\alpha \not\equiv 0 \mod 1 \\ 1 & ,\alpha \equiv 0 \mod 1 \end{cases}$$

For $n = 1$, we will write χ_α for $\chi_{\alpha,1}$

Lemma 5. *If $(q-1)\alpha \equiv 0 \mod 1$, then $\chi_{\alpha,n} = \chi_\alpha(\mathbb{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x))$*

Proof. $\chi_{\alpha,n}(x) = \phi(x)^{(q^n-1)\alpha} = \left(\phi(x)^{(q-1)\alpha}\right)^{1+q+q^2+\cdots+q^{n-1}} = \chi_\alpha(x^{1+q+q^2+\cdots+q^{n-1}}) = \chi_\alpha(\mathbb{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x))$. □

Proposition 6. *The number of solutions to the equation $x^n = u$ in $\mathbb{F}_q$, denoted by $N(u)$ is given by $\displaystyle\sum_{d\alpha\equiv 0 \mod 1} \chi_\alpha(u)$.*

Proof. When $u = 0$, then both sides become 1. When $u \neq 0$, then we observe that the right hand side is $\displaystyle\sum_{\nu=0}^{d-1} \chi_{1/d}(u)^\nu$. So, $\chi_{1/d}(u)$ is then a d-th root of unity if and only if u is a d-th power in $\mathbb{F}_q^\times$. This completes the proof. □

Using this result, we have

$$N = \sum_{\substack{\alpha=(\alpha_0,\dots,\alpha_r) \\ d_i\alpha_i \equiv 0 \mod 1}} \sum_{\substack{u=(u_0,\dots,u_r) \\ L(u)=0}} \chi_{\alpha_0}(u_0)\cdots\chi_{\alpha_r}(u_r) \tag{3}$$

Notice that $L(u) = 0$ has q^r points, and thus the inner sum amounts to q^r when $\alpha_0 = \cdots = \alpha_r = 0$. In fact, if some, but not all, of the α_i's are 0, then the sum amounts to 0. To see this, suppose $\alpha_0, \dots, \alpha_{s-1}$ are the non-zero ones and $\alpha_s, \dots, \alpha_r = 0$. Then, $L(u) = 0$ has q^{r-s} points and the double summation becomes

$$q^{r-s} \prod_{i=0}^{s-1} \left(\sum_{u_i} \chi_{\alpha_i}(u_i) \right) \tag{4}$$

and the claim follows from orthogonality of characters. Hence, converts to

$$N = q^r + \sum_{\substack{\alpha=(\alpha_0,\dots,\alpha_r) \\ d_i\alpha_i \equiv 0 \mod 1 \\ 0<\alpha_i<1}} \sum_{\substack{u=(u_0,\dots,u_r) \\ L(u)=0}} \chi_{\alpha_0}(u_0)\cdots\chi_{\alpha_r}(u_r) \tag{5}$$

We can rewrite the inner sum in a cleaner way. Clearly, the $u_0 = 0$ terms contribute nothing to the sum. So, just assume $u_0 \neq 0$, and let $u_i = u_0 v_i$ for some $v_i \in \mathbb{F}_q$. Then,

$$\sum_{\substack{u=(u_0,\dots,u_r) \\ u_0+u_1+\cdots+u_r=0}} \chi_{\alpha_0}(u_0)\cdots\chi_{\alpha_r}(u_r) = \sum_{u_0 \neq 0} \chi_{\alpha_0+\cdots+\alpha_r}(u_0) \sum_{1+v_1+\cdots+v_r=0} \chi_{\alpha_1}(v_1)\cdots\chi_{\alpha_r}(v_r)$$

Now, depending on whether $\alpha_0 + \cdots + \alpha_r \equiv 0 \mod 1$, the outer sum is $q-1$ and 0 respectively.

4 Gauss and Jacobi Sums

This section follows [Wei49]. If you want to read more about Gauss and Jacobi sums, please refer to [Con][IR90].

Now, for $\alpha_i(q-1)$, $\alpha_i \not\equiv 0 \mod 1$, and $\alpha_1 + \cdots + \alpha_r \equiv 0 \mod 1$ we can define

Definition 7 (Jacobi sums)**.**

$$\begin{aligned} j(\alpha) &:= \sum_{1+v_1+\cdots+v_r=0} \chi_{\alpha_1}(v_1)\cdots\chi_{\alpha_r}(v_r) \\ &= \frac{1}{q-1} \sum_{u_0+u_1+\cdots+u_r=0} \chi_{\alpha_0}(u_0)\cdots\chi_{\alpha_r}(u_r) \end{aligned}$$

In terms of Jacobi sums, we can write the number of solutions N of (1) by

$$N = q^r + (q-1) \sum_{\substack{\alpha=(\alpha_0,\dots,\alpha_r) \\ d_i\alpha_i \equiv 0 \mod 1 \\ 0<\alpha_i<1 \\ \alpha_0+\cdots+\alpha_r=0}} \chi_{\alpha_0}(a_0^{-1}) \cdots \chi_{\alpha_r}(a_r^{-1}) j(\alpha) \tag{6}$$

These Jacobi sums are closely related to other sums called Gauss sums. We will use Gauss sums to compute Jacobi sums further.

Definition 8. *Define* $\psi_q : \mathbb{F}_q \to \mathbb{C}^\times$ *by*

$$\psi_q(a) = e^{2\pi i \frac{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a)}{p}}$$

Proposition 9. *The character* ψ_q *is not trivial, and every additive character of* $\mathbb{F}_q$ *is of the form* $a \mapsto \psi_q(ca)$ *for some* $c \in \mathbb{F}_q$.

Proof. This follows from Artin's theorem on linear independence of characters. □

Definition 10. *Let* $\chi : \mathbb{F}_q \to \mathbb{C}$ *be any of the multiplicative character of* $\mathbb{F}_q$ *and* ψ_q *as defined earlier. Then, the Gauss sum* $g(\chi)$ *is*

$$g(\chi) := \sum_{x \in \mathbb{F}_q} \chi(x)\psi_q(x) \tag{7}$$

It is easy to see that if χ is the trivial character then $g(\chi) = 0$. So suppose $\chi \neq \mathbf{1}$. Then,

Proposition 11.

$$g(\chi)\overline{g}(\chi) = q$$

Proof.

$$\begin{aligned} g(\chi)\overline{g}(\chi) &= \sum_{y \in \mathbb{F}_q} \sum_{x \in \mathbb{F}_q} \chi(xy^{-1})\psi_q(x-y) \\ &= \sum_{x \in \mathbb{F}_q} \chi(x) \sum_{y \in \mathbb{F}_q} \psi_q((x-1)y) \\ &= \sum_{0 \neq x \in \mathbb{F}_q} \chi(x) \sum_{0 \neq y \in \mathbb{F}_q} \psi_q((x-1)y) \\ &= \chi(1) \sum_{y \neq 0} 1 + \sum_{x \neq 0,1} \chi(x)(-1) \\ &= q - 1 + (-1)(-1) \\ &= q \end{aligned}$$

□

Now, for $t \neq 0$, if we replace x in $g(\chi)$ by tx, we get

$$g(\chi) = \chi(t) \sum_{x \in \mathbb{F}_q} \chi(x) \psi_q(tx)$$

Using the previous proposition, and interchanging t and x we have

$$\chi(x) = \frac{g(\chi)}{q} \sum_{t \in \mathbb{F}_q} \overline{\chi}(t) \overline{\psi}_q(tx) \tag{8}$$

Remark 12. *You can see this as the Fourier expansion of χ with respect to the additive characters ψ_q.*

Using this in the definition of Jacobi sums, we have

$$\begin{aligned} j(a) &= \frac{1}{q-1} \sum_{u_0+u_1+\cdots+u_r=0} \chi_{\alpha_0}(u_0) \cdots \chi_{\alpha_r}(u_r) \\ &= \frac{1}{q^{r+1}} g(\chi_{\alpha_0}) \cdots g(\chi_{\alpha_r}) \sum_t \overline{\chi}_{\alpha_0}(t_0) \cdots \overline{\chi}_{\alpha_r}(t_r) \sum_{u_0+\cdots+u_r=0} \overline{\psi} \left(\sum_i t_i u_i \right) \end{aligned}$$

The inner sum being a character sum on the vector space $(u_0, \ldots, u_r)$ satisfying $u_0 + \cdots + u_r = 0$ with q^r elements is either q^r or 0 depending on whether $\overline{\psi}$ is trivial or not. The former case happens if and only if all t_i's are equal. Indeed, otherwise we can solve equations like $\sum u_i = 0$ and $\sum t_i u_i = s$ with $s \in \mathbb{F}_q$. Since we have $\alpha_0 + \cdots + \alpha_r \equiv 0 \mod 1$ by definition of Jacobi sums, we can deduce that

$$j(a) = \frac{1}{q} g(\chi_{\alpha_0}) \cdots g(\chi_{\alpha_r})$$

After this we are interested to see what happens to the number of solutions when we move from $\mathbb{F}_q$ to an extension $\mathbb{F}_{q^\nu}$ for some positive integer ν. To address this question, we will need an important result of Davenport and Hasse.

Theorem 13 (Davenport-Hasse theorem)**.**

$$-g(\chi_{\alpha,\nu}) = (-g(\chi_\alpha))^\nu$$

Proof. [Wei49][IR90] □

Let N_ν be the number of solutions of equation (1) in the field $\mathbb{F}_{q^\nu}$. Consider (1) as the equation of a variety in the projective space $\mathbb{P}^r$ of dimension r over $\mathbb{F}_q$. Let $\overline{N}$ be the number of solutions in the projective space, it is related to the number of solutions on the affine space by $\overline{N}(q-1)+1 = N$. Now, plugging this into we get

(9)
$$\overline{N} = 1 + q + \cdots + q^{r-1} + \sum_{\substack{\alpha=(\alpha_0,\ldots,\alpha_r) \\ d_i\alpha_i \equiv 0 \mod 1 \\ 0<\alpha_i<1 \\ \alpha_0+\cdots+\alpha_r\equiv 0 \pmod 1}} \overline{\chi}_{\alpha_0}(a_0)\cdots\overline{\chi}_{\alpha_r}(a_r)j(\alpha)$$

Now, if $\overline{N}_\nu$ is the number of points on the variety over $\mathbb{F}_{q^\nu}$, we shall calculate the series

$$\sum_{\nu=1}^{\infty} \overline{N}_\nu U^{\nu-1}$$

5 Weil conjectures

We will see how to do this in the special case of (1) when $n_1 = \cdots = n_r = n$. Suppose $n\alpha_i \equiv 0 \mod 1, \alpha_0 + \cdots + \alpha_r \equiv 0 \mod 1, 0 < \alpha_i < 1$. Let

$$\mu = \mu(\alpha) = \min\{\mu : (q^\mu - 1)\alpha_i \equiv 0 \mod 1\ \forall\ 0 \leqslant i \leqslant r\}$$

The extension $\mathbb{F}_{q^\nu}$ such that $(q^\nu - 1)\alpha_i \equiv 0 \mod 1$ are those for which ν is a multiple of μ and in fact, those are all of them. Choosing a generator for $\mathbb{F}_{q^\mu}$ we can define the characters χ_{α_i}, the Gauss sums $g(\chi_{\alpha_i})$ and the Jacobi sums $j(\alpha)$. After this, let $\chi_{\alpha_i,\lambda\mu}, g(\chi_{\alpha_i,\lambda\mu}), j_{\lambda\mu}(\alpha)$ the corresponding objects in the extension $\mathbb{F}_{q^{\nu\mu}}$. From Davenport-Hasse's theorem and basic checking, we have

(1) $\chi_{\alpha_i,\lambda\mu} = \chi_{\alpha_i}(a_i)^\lambda$
(2) $g(\chi_{\alpha_i,\lambda\mu}) = (-1)^{\lambda-1} g(\chi_{\alpha_i})^\lambda$
(3) $j_{\lambda\mu}(\alpha) = (-1)^{(\lambda-1)(r-1)} j(a)^\lambda$

So,

(10)
$$\overline{N}_\nu = 1 + q^\nu + \cdots + q^{\nu(r-1)} + \sum_{\substack{\alpha=(\alpha_0,\ldots,\alpha_r) \\ d_i\alpha_i \equiv 0 \mod 1 \\ 0<\alpha_i<1 \\ \alpha_0+\cdots+\alpha_r\equiv 0 \pmod 1}} \chi_{\alpha_0,\nu}(a_0^{-1})\cdots\chi_{\alpha_r,\nu}(a_r^{-1})j_\nu(\alpha)$$

with $\nu = \lambda\mu$. We let $q = q^\mu$ for simplicity of notation. Then, the previous equation becomes (after possibly putting $\nu = \lambda$)

(11)
$$\overline{N}_\nu = 1 + q^\nu + \cdots + q^{\nu(r-1)} + \sum_{\substack{\alpha=(\alpha_0,\ldots,\alpha_r) \\ d_i\alpha_i \equiv 0 \mod 1 \\ 0<\alpha_i<1 \\ \alpha_0+\cdots+\alpha_r\equiv 0 \pmod 1}} (-1)^{(\nu-1)(r-1)} \left(\chi_{\alpha_0}(a_0^{-1})\cdots\chi_{\alpha_r}(a_r^{-1})j(\alpha)\right)^\nu$$

Using the identity

$$\sum_{\nu=1}^{\infty} X^{\nu} U^{\nu-1} = \frac{d}{dU}(-\log(1-XU))$$

we have

$$\sum_{\nu=1}^{\infty} \overline{N}_{\nu} U^{\nu-1} = \sum_{i=0}^{r-1} \frac{d}{dU}(-\log(1-q^{i}U)) + (-1)^{r} \sum_{\alpha} \frac{1}{\mu(\alpha)} \frac{d}{dU}(-\log(1-C(\alpha)U^{\mu(\alpha)})$$

where $C(\alpha) = (-1)^{r-1}\chi_{\alpha_0}(a_0^{-1}) \cdots \chi_{\alpha_r}(a_r^{-1}) j(\alpha)$

Note that the map $x \mapsto a^{q}$ is an automorphism of $\mathbb{F}_{q^{\mu}}$ which leaves a_i unchanged. Thus, $C(q\alpha) = C(\alpha)$. Thus, in the last sum, the terms corresponding to the sets α and $q^{\nu}\alpha$ with $0 \leqslant \nu \leqslant \mu - 1$ are the same and there are $\mu(\alpha)$ many of them, and hence we can cancel the $\mu(\alpha)$.

Definition 14. *Let V be a variety without singular points, of dimension n, defined over a finite field with q elements. Let $\overline{N}_{\nu}$ be the number of rational points on V over the extension $\mathbb{F}_{q^{\nu}}$ of $\mathbb{F}_q$. Then, we define*

$$\mathfrak{Z}(V,U) := \exp\left(\sum_{\nu=1}^{\infty} \overline{N}_{k} \frac{U^{\nu}}{\nu}\right)$$

From the above discussion, we have

$$\mathfrak{Z}(V,U) = \frac{P(U)^{(-1)^{r}}}{(1-U)(1-qU)\cdots(1-q^{r-1}U)}$$

with $P(U) = \prod_{\alpha}(1 - C(\alpha)U)$.

Weil conjectures the following:

Theorem 15 (Weil's conjectures)**.** *Let V be a variety without singular points, and of dimension n. Then,*

(1) *(Rationality) $\mathfrak{Z}(V,U)$ is a rational function.*
(2) *(Functional equation) The function $\mathfrak{Z}(V,U)$ satisfies the functional equation*

$$\mathfrak{Z}(V, \frac{1}{q^{n}U}) = \epsilon q^{n\chi/2} U^{\chi} \mathfrak{Z}(V,U)$$

where $\epsilon = \pm 1$ and χ is the Euler-Poincaré characteristic of V (intersection number of the diagonal with itself on the product $V \times V$).
(3) *(Riemann Hypothesis) One can write*

$$\mathfrak{Z}(V,U) = \frac{P_1(U)P_3(U)\cdots P_{2n-1}(U)}{P_0(U)P_2(U)\cdots P_{2n}(U)}$$

where $P_0(U) = 1 - U$, $P_{2n}(U) = 1 - q^n U$ *and for* $1 \leqslant h \leqslant 2n-1$ *we have*

$$P_h(U) = \prod_{i=1}^{B_h} (1 - \alpha_{h,i} U)$$

where $\alpha_{h,i}$ *are algebraic integers with absolute value* $q^{h/2}$.

(4) *The degree* B_h *of* P_h *called the Betti numbers of the variety* B. *Then, the Euler-Poincaré characteristic* χ *can be expressed by*

$$\chi = \sum_h (-1)^h B_h$$

6 History of Weil conjectures and literature

While writing this section, I realised that I cannot do much justice due to my very limited knowledge. I shall instead share this wonderful commentary written by M. Goresky [Gor18], and also refer to the notes by Tamás Szamuely click here for a proper timeline of the progress on the conjectures. I also found the notes by Hindry [Hin12] (in french) very helpful while preparing for this talk.

References

[Con] Keith Conrad. URL: https://kconrad.math.uconn.edu/blurbs/gradnumthy/Gauss-Jacobi-sums.pdf.

[Del77] P. Deligne. *Cohomologie étale*. Vol. 569. Lecture Notes in Mathematics. Séminaire de géométrie algébrique du Bois-Marie SGA $4\frac{1}{2}$. Springer-Verlag, Berlin, 1977, pp. iv+312. ISBN: 3-540-08066-X; 0-387-08066-X. DOI: 10.1007/BFb0091526. URL: https://doi.org/10.1007/BFb0091526.

[Dwo60] Bernard Dwork. "On the rationality of the zeta function of an algebraic variety". In: *Amer. J. Math.* 82 (1960), pp. 631–648. ISSN: 0002-9327,1080-6377. DOI: 10.2307/2372974. URL: https://doi.org/10.2307/2372974.

[Gor18] Mark Goresky. "Commentary on "Numbers of solutions of equations in finite fields" by André Weil". In: *Bull. Amer. Math. Soc. (N.S.)* 55.3 (2018), pp. 327–329. ISSN: 0273-0979,1088-9485. DOI: 10.1090/bull/1617. URL: https://doi.org/10.1090/bull/1617.

[Gro60] Alexander Grothendieck. "The cohomology theory of abstract algebraic varieties". In: *Proc. Internat. Congress Math. 1958*. Cambridge Univ. Press, New York, 1960, pp. 103–118.

[Hin12] Marc Hindry. "La preuve par André Weil de l'hypothèse de Riemann pour une courbe sur un corps fini". In: *Henri Cartan & André Weil, mathématiciens du XX^e siècle*. Ed. Éc. Polytech., Palaiseau, 2012, pp. 63–98. ISBN: 978-2-7302-1610-4.

[IR90] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*. en. Vol. 84. Graduate Texts in Mathematics. New York, NY: Springer New York, 1990. ISBN: 9781441930941 9781475721034. DOI: 10.1007/978-1-4757-2103-4. URL: http://link.springer.com/10.1007/978-1-4757-2103-4.

[M A73] J. L. Verdier M. Artin A. Grothendieck. *Théorie des topos et cohomologie étale des schémas. Tome 3*. Vol. Vol. 305. Lecture Notes in Mathematics. Séminaire de Géométrie Algébrique du Bois-Marie 1963–1964 (SGA 4), Dirigé par M. Artin, A. Grothendieck et J. L. Verdier. Avec la collaboration de P. Deligne et B. Saint-Donat. Springer-Verlag, Berlin-New York, 1973, pp. vi+640.

[Ser58] Jean-Pierre Serre. "Sur la topologie des variétés algébriques en caractéristique p". In: *Symposium internacional de topología algebraica International symposium on algebraic topology*. Universidad Nacional Autónoma de México and UNESCO, México, 1958, pp. 24–53.

[Wei48] André Weil. *Sur les courbes algébriques et les variétés qui s'en déduisent*. Vol. 7 (1945). Publications de l'Institut de Mathématiques de l'Université de Strasbourg [Publications of the Mathematical Institute of the University of Strasbourg]. Actualités Scientifiques et Industrielles, No. 1041. [Current Scientific and Industrial Topics]. Hermann & Cie, Paris, 1948, pp. iv+85.

[Wei49] André Weil. "Numbers of solutions of equations in finite fields". In: *Bulletin of the American Mathematical Society* 55.5 (1949), pp. 497–508.

[Wei56] André Weil. "Abstract versus classical algebraic geometry". In: *Proceedings of the International Congress of Mathematicians, 1954, Amsterdam, vol. III*. Erven P. Noordhoff N. V., Groningen, 1956, pp. 550–558.