

$\phi(x) = (x)$ dla $x \in \mathbb{Z}$, $\forall q \in \mathbb{N}$

WYKŁAD

Algorytm AKS : Agrawal, Kayal, Saxena, 2004

Dane: $n \in \mathbb{N}$

Pkt. czy $n \in P?$

prof. Kacper Gąsiorek
studenci

Pierwszy det. alg. w PTMFE, bez złożenia (były chyba, ale np. przy
zat. nie hip. Ramanu
9 stron, 1,5 wstęp, 1,5 bibliografia (zadoduszka
wzorowana)

Po poprawach \rightarrow w ogóle alg. elementarna, ujemnej pracy.

(nie zidentyfikowano praktyce, bo np. test Miller-Rabin działa
mniej skutecznie w $O(n^3)$ i z góry daje dobry wynik.)

Ten $O(n^{15/2})$ przy zat. hipotezy Sophie Germain o ogólnie
Tn $O(n^{2/2})$. Wszystko

Główna idea (zagłówkowe MTF): Jest modyf. co dwa kroki
 $O(n^6)$.

Lemat 1: Niech $a \in \mathbb{Z}$, $n \in \mathbb{N}$, $n \geq 2$, $a \neq n$. Wtedy $n \in P$ wtedy i tylko wtedy, gdy

$\exists x \in \mathbb{Z} \quad (x+a)^n \equiv x^n + a \pmod{n}$

$$(x+a)^n \equiv x^n + a \pmod{n}$$

D-d

zaznaczamy (x, n) i (a, n) wtedy i tylko wtedy, gdy

\Rightarrow Niech $n \in P$. Przy $x^n \equiv 1 \pmod{n}$

Przy $x^n \equiv a^n \pmod{n}$ dla $a \in \mathbb{Z}$ MTF mamy, że $p | a - a$, czyli OK.

$$\text{Przy } x^n \equiv a^n \pmod{n} \quad \binom{n}{a} = \frac{n!}{a!(n-a)!}$$

zatem zrobacyd, że $n \mid \binom{n}{a}$, nie dalej mówiąc, a dalej literacki.

\Leftarrow Niech $n \in P$. Niech $q \mid n$ i $q^k \mid n$, ale $q^{k+1} \nmid n$.

$$\text{Rozważmy } \binom{n}{q} = \frac{n!}{q!(n-q)!} = \frac{n!}{q!} \cdot \frac{(n-q)!}{(n-q)!} \cdot \frac{q^k}{n} \mid n^{\frac{n}{q}}, \text{ ale } q^{k+1} \nmid n^{\frac{n}{q}}.$$

$q \mid q!$, czyli $q^k \nmid \binom{n}{q}$

$$\text{Czyli } n \nmid \binom{n}{q}.$$

Jednak spr. czg $(x+a)^n = x^n + a \pmod{n}$
tak po prostu zapiszby $O(n)$ czasem

Ponadto: sprawdzać to modulo $(x^v - 1)$ dla odpowiednio
dobrych v oraz x . Później, że dla ist. dorygo
znowu to wystarczy i da się zrobić w PTIME.

Rzgl. a modulo r to najmniejsze $k \geq 0$ dla $a^k \equiv 1 \pmod{r}$.

Twierdzenie Eulera: $\phi(r) = |\{x \in \mathbb{Z}_r : x \perp r\}|$.

Skoro $a^{\phi(r)} \equiv 1 \pmod{r}$, to $\phi(r) > \log n$.

Skoro $a^{\phi(r)} \equiv 1 \pmod{r}$, to $a^{\phi(r)} \equiv 1 \pmod{r}$.

ALGORYTM

1. Jeśli $n = a^b$ dla $a \in \mathbb{N}, b \geq 1$ to ZtożNA

2. Znajdi największe $r \geq 0$ $\phi(r) > \log n$.

3. Jeśli $1 \leq (a, n) \leq n$ dla pewnego $a \in \mathbb{N}$ to ZtożNA

4. Jeśli $n \leq r$ to PIERWSZA (\Rightarrow)

5. Dla $a=1$ do $\lceil \sqrt{\phi(r)} \cdot \log n \rceil$ rob

jeśli $(x+a)^n \neq x^n + a \pmod{x^r - 1, n}$ to ZtożNA

6. PIERWSZA

Fakt 1

Jednakże niepotrzebna, to algorytmu funkcja sprawdzająca jest

D-d

Jakoże nie może zatrzymać się 1, 3, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 107, 113, 127, 131, 137, 149, 151, 157, 163, 173, 179, 181, 191, 197, 199, 211, 223, 227, 233, 239, 241, 251, 257, 263, 271, 281, 283, 293, 307, 311, 313, 317, 331, 347, 353, 359, 367, 373, 383, 389, 397, 401, 409, 419, 431, 433, 437, 443, 457, 463, 467, 479, 487, 491, 499, 503, 521, 523, 541, 547, 557, 563, 569, 571, 587, 593, 601, 613, 617, 623, 631, 643, 647, 653, 661, 673, 683, 691, 697, 701, 709, 713, 721, 733, 743, 751, 761, 769, 773, 787, 791, 797, 803, 811, 823, 833, 841, 853, 863, 871, 883, 891, 897, 901, 913, 923, 931, 941, 953, 961, 971, 983, 991, 1001, 1013, 1023, 1031, 1041, 1053, 1061, 1073, 1081, 1091, 1103, 1111, 1123, 1131, 1141, 1153, 1161, 1173, 1181, 1191, 1201, 1213, 1223, 1231, 1241, 1253, 1261, 1273, 1281, 1291, 1301, 1313, 1321, 1331, 1341, 1353, 1361, 1373, 1381, 1391, 1401, 1413, 1421, 1431, 1441, 1453, 1461, 1473, 1481, 1491, 1501, 1513, 1521, 1531, 1541, 1553, 1561, 1573, 1581, 1591, 1601, 1613, 1621, 1631, 1641, 1653, 1661, 1673, 1681, 1691, 1701, 1713, 1721, 1731, 1741, 1753, 1761, 1773, 1781, 1791, 1801, 1813, 1821, 1831, 1841, 1853, 1861, 1873, 1881, 1891, 1901, 1913, 1921, 1931, 1941, 1953, 1961, 1973, 1981, 1991, 2001, 2013, 2021, 2031, 2041, 2053, 2061, 2073, 2081, 2091, 2101, 2113, 2121, 2131, 2141, 2153, 2161, 2173, 2181, 2191, 2201, 2213, 2221, 2231, 2241, 2253, 2261, 2273, 2281, 2291, 2301, 2313, 2321, 2331, 2341, 2353, 2361, 2373, 2381, 2391, 2401, 2413, 2421, 2431, 2441, 2453, 2461, 2473, 2481, 2491, 2501, 2513, 2521, 2531, 2541, 2553, 2561, 2573, 2581, 2591, 2601, 2613, 2621, 2631, 2641, 2653, 2661, 2673, 2681, 2691, 2701, 2713, 2721, 2731, 2741, 2753, 2761, 2773, 2781, 2791, 2801, 2813, 2821, 2831, 2841, 2853, 2861, 2873, 2881, 2891, 2901, 2913, 2921, 2931, 2941, 2953, 2961, 2973, 2981, 2991, 3001, 3013, 3021, 3031, 3041, 3053, 3061, 3073, 3081, 3091, 3101, 3113, 3121, 3131, 3141, 3153, 3161, 3173, 3181, 3191, 3201, 3213, 3221, 3231, 3241, 3253, 3261, 3273, 3281, 3291, 3301, 3313, 3321, 3331, 3341, 3353, 3361, 3373, 3381, 3391, 3401, 3413, 3421, 3431, 3441, 3453, 3461, 3473, 3481, 3491, 3501, 3513, 3521, 3531, 3541, 3553, 3561, 3573, 3581, 3591, 3601, 3613, 3621, 3631, 3641, 3653, 3661, 3673, 3681, 3691, 3701, 3713, 3721, 3731, 3741, 3753, 3761, 3773, 3781, 3791, 3801, 3813, 3821, 3831, 3841, 3853, 3861, 3873, 3881, 3891, 3901, 3913, 3921, 3931, 3941, 3953, 3961, 3973, 3981, 3991, 4001, 4013, 4021, 4031, 4041, 4053, 4061, 4073, 4081, 4091, 4101, 4113, 4121, 4131, 4141, 4153, 4161, 4173, 4181, 4191, 4201, 4213, 4221, 4231, 4241, 4253, 4261, 4273, 4281, 4291, 4301, 4313, 4321, 4331, 4341, 4353, 4361, 4373, 4381, 4391, 4401, 4413, 4421, 4431, 4441, 4453, 4461, 4473, 4481, 4491, 4501, 4513, 4521, 4531, 4541, 4553, 4561, 4573, 4581, 4591, 4601, 4613, 4621, 4631, 4641, 4653, 4661, 4673, 4681, 4691, 4701, 4713, 4721, 4731, 4741, 4753, 4761, 4773, 4781, 4791, 4801, 4813, 4821, 4831, 4841, 4853, 4861, 4873, 4881, 4891, 4901, 4913, 4921, 4931, 4941, 4953, 4961, 4973, 4981, 4991, 5001, 5013, 5021, 5031, 5041, 5053, 5061, 5073, 5081, 5091, 5101, 5113, 5121, 5131, 5141, 5153, 5161, 5173, 5181, 5191, 5201, 5213, 5221, 5231, 5241, 5253, 5261, 5273, 5281, 5291, 5301, 5313, 5321, 5331, 5341, 5353, 5361, 5373, 5381, 5391, 5401, 5413, 5421, 5431, 5441, 5453, 5461, 5473, 5481, 5491, 5501, 5513, 5521, 5531, 5541, 5553, 5561, 5573, 5581, 5591, 5601, 5613, 5621, 5631, 5641, 5653, 5661, 5673, 5681, 5691, 5701, 5713, 5721, 5731, 5741, 5753, 5761, 5773, 5781, 5791, 5801, 5813, 5821, 5831, 5841, 5853, 5861, 5873, 5881, 5891, 5901, 5913, 5921, 5931, 5941, 5953, 5961, 5973, 5981, 5991, 6001, 6013, 6021, 6031, 6041, 6053, 6061, 6073, 6081, 6091, 6101, 6113, 6121, 6131, 6141, 6153, 6161, 6173, 6181, 6191, 6201, 6213, 6221, 6231, 6241, 6253, 6261, 6273, 6281, 6291, 6301, 6313, 6321, 6331, 6341, 6353, 6361, 6373, 6381, 6391, 6401, 6413, 6421, 6431, 6441, 6453, 6461, 6473, 6481, 6491, 6501, 6513, 6521, 6531, 6541, 6553, 6561, 6573, 6581, 6591, 6601, 6613, 6621, 6631, 6641, 6653, 6661, 6673, 6681, 6691, 6701, 6713, 6721, 6731, 6741, 6753, 6761, 6773, 6781, 6791, 6801, 6813, 6821, 6831, 6841, 6853, 6861, 6873, 6881, 6891, 6901, 6913, 6921, 6931, 6941, 6953, 6961, 6973, 6981, 6991, 7001, 7013, 7021, 7031, 7041, 7053, 7061, 7073, 7081, 7091, 7101, 7113, 7121, 7131, 7141, 7153, 7161, 7173, 7181, 7191, 7201, 7213, 7221, 7231, 7241, 7253, 7261, 7273, 7281, 7291, 7301, 7313, 7321, 7331, 7341, 7353, 7361, 7373, 7381, 7391, 7401, 7413, 7421, 7431, 7441, 7453, 7461, 7473, 7481, 7491, 7501, 7513, 7521, 7531, 7541, 7553, 7561, 7573, 7581, 7591, 7601, 7613, 7621, 7631, 7641, 7653, 7661, 7673, 7681, 7691, 7701, 7713, 7721, 7731, 7741, 7753, 7761, 7773, 7781, 7791, 7801, 7813, 7821, 7831, 7841, 7853, 7861, 7873, 7881, 7891, 7901, 7913, 7921, 7931, 7941, 7953, 7961, 7973, 7981, 7991, 8001, 8013, 8021, 8031, 8041, 8053, 8061, 8073, 8081, 8091, 8101, 8113, 8121, 8131, 8141, 8153, 8161, 8173, 8181, 8191, 8201, 8213, 8221, 8231, 8241, 8253, 8261, 8273, 8281, 8291, 8301, 8313, 8321, 8331, 8341, 8353, 8361, 8373, 8381, 8391, 8401, 8413, 8421, 8431, 8441, 8453, 8461, 8473, 8481, 8491, 8501, 8513, 8521, 8531, 8541, 8553, 8561, 8573, 8581, 8591, 8601, 8613, 8621, 8631, 8641, 8653, 8661, 8673, 8681, 8691, 8701, 8713, 8721, 8731, 8741, 8753, 8761, 8773, 8781, 8791, 8801, 8813, 8821, 8831, 8841, 8853, 8861, 8873, 8881, 8891, 8901, 8913, 8921, 8931, 8941, 8953, 8961, 8973, 8981, 8991, 9001, 9013, 9021, 9031, 9041, 9053, 9061, 9073, 9081, 9091, 9101, 9113, 9121, 9131, 9141, 9153, 9161, 9173, 9181, 9191, 9201, 9213, 9221, 9231, 9241, 9253, 9261, 9273, 9281, 9291, 9301, 9313, 9321, 9331, 9341, 9353, 9361, 9373, 9381, 9391, 9401, 9413, 9421, 9431, 9441, 9453, 9461, 9473, 9481, 9491, 9501, 9513, 9521, 9531, 9541, 9553, 9561, 9573, 9581, 9591, 9601, 9613, 9621, 9631, 9641, 9653, 9661, 9673, 9681, 9691, 9701, 9713, 9721, 9731, 9741, 9753, 9761, 9773, 9781, 9791, 9801, 9813, 9821, 9831, 9841, 9853, 9861, 9873, 9881, 9891, 9901, 9913, 9921, 9931, 9941, 9953, 9961, 9973, 9981, 9991, 10001, 10013, 10021, 10031, 10041, 10053, 10061, 10073, 10081, 10091, 10101, 10113, 10121, 10131, 10141, 10153, 10161, 10173, 10181, 10191, 10201, 10213, 10221, 10231, 10241, 10253, 10261, 10273, 10281, 10291, 10301, 10313, 10321, 10331, 10341, 10353, 10361, 10373, 10381, 10391, 10401, 10413, 10421, 10431, 10441, 10453, 10461, 10473, 10481, 10491, 10501, 10513, 10521, 10531, 10541, 10553, 10561, 10573, 10581, 10591, 10601, 10613, 10621, 10631, 10641, 10653, 10661, 10673, 10681, 10691, 10701, 10713, 10721, 10731, 10741, 10753, 10761, 10773, 10781, 10791, 10801, 10813, 10821, 10831, 10841, 10853, 10861, 10873, 10881, 10891, 10901, 10913, 10921, 10931, 10941, 10953, 10961, 10973, 10981, 10991, 11001, 11013, 11021, 11031, 11041, 11053, 11061, 11073, 11081, 11091, 11101, 11113, 11121, 11131, 11141, 11153, 11161, 11173, 11181, 11191, 11201, 11213, 11221, 11231, 11241, 11253, 11261, 11273, 11281, 11291, 11301, 11313, 11321, 11331, 11341, 11353, 11361, 11373, 11381, 11391, 11401, 11413, 11421, 11431, 11441, 11453, 11461, 11473, 11481, 11491, 11501, 11513, 11521, 11531, 11541, 11553, 11561, 11573, 11581, 11591, 11601, 11613, 11621, 11631, 11641, 11653, 11661, 11673, 11681, 11691, 11701, 11713, 11721, 11731, 11741, 11753, 11761, 11773, 11781, 11791, 11801, 11813, 11821, 11831, 11841, 11853, 11861, 11873, 11881, 11891, 11901, 11913, 11921, 11931, 11941, 11953, 11961, 11973, 11981, 11991, 12001, 12013, 12021, 12031, 12041, 12053, 12061, 12073, 12081, 12091, 12101, 12113, 12121, 12131, 12141, 12153, 12161, 12173, 12181, 12191, 12201, 12213, 12221, 12231, 12241, 12253, 12261, 12273, 12281, 12291, 12301, 12313, 12321, 12331, 12341, 12353, 12361, 12373, 12381, 12391, 12401, 12413, 12421, 12431, 12441, 12453, 12461, 12473, 12481, 12491, 12501, 12513, 12521, 12531, 12541, 12553, 12561, 12573, 12581, 12591, 12601, 12613, 12621, 12631, 12641, 12653, 12661, 12673, 12681, 12691, 12701, 12713, 12721, 12731, 12741, 12753, 12761, 12773, 12781, 12791, 12801, 12813, 12821, 12831, 12841, 12853, 12861, 12873, 12881, 12891, 12901, 12913, 12921, 12931, 12941, 12953, 12961, 12973, 12981, 12991, 13001, 13013, 13021, 13031, 13041, 13053, 13061, 13073, 13081, 13091, 13101, 13113, 13121, 13131, 13141, 13153, 13161, 13173, 13181, 13191, 13201, 13213, 13221, 13231, 13241, 13253, 13261, 13273, 13281, 13291, 13301, 13313, 13321, 13331, 13341, 13353, 13361, 13373, 13381, 13391, 13401, 13413, 13421, 13431, 13441, 13453, 13461, 13473, 13481, 13491, 13501, 13513, 13521, 13531, 13541, 13553, 13561, 13573, 13581, 13591, 13601, 13613, 13621, 13631, 13641, 13653, 13661, 13673, 13681, 13691, 13701, 13713, 13721, 13731, 13741, 13753, 13761, 13773, 13781, 13791, 13801, 13813, 13821, 13831, 13841, 13853, 13861, 13873, 13881, 13891, 13901, 13913, 13921, 13931, 13941, 13953, 13961, 13973, 13981, 13991, 14001, 14013, 14021, 14031, 14041, 14053, 14061, 14073, 14081, 14091, 14101, 14113, 14121, 14131, 14141, 14153, 14161, 14173, 14181, 14191, 14201, 14213, 14221, 14231, 14241, 14253, 14261, 14273, 14281, 14291, 14301, 14313, 14321, 14331, 14341, 14353, 14361, 14373, 14381, 14391, 14401, 14413, 14421, 14431, 14441, 14453, 14461, 14473, 14481, 14491, 14501, 14513, 14521, 14531, 14541, 14553, 14561, 14573, 14581, 14591, 14601, 14613, 14621, 14631, 14641, 14653, 14661, 14673, 14681, 14691, 14701, 14713, 14721, 14731, 14741, 14753, 14761, 14773, 14781, 14791, 14801, 14813, 14821, 14831, 14841, 14853, 14861, 14873, 14881, 14891, 14901, 14913, 14921, 14931, 14941, 14953, 14961, 14973, 14981, 14991, 15001, 15013, 15021, 15031, 15041, 15053, 15061, 15073, 15081, 15091, 15101, 15113, 15121, 15131, 15141, 15153, 15161, 15173, 15181, 15191, 15201, 15213, 15221, 15231, 15241, 15253, 15261, 15273, 15281, 15291, 15301, 15313, 15321, 15331, 15341, 15353, 15361, 15373, 15381, 15391, 15401, 15413, 15421, 15431, 15441, 15453, 15461, 15473, 15481, 15491, 15501, 15513, 15521, 15531, 15541, 15553, 15561, 15573, 15581, 15591, 15601, 15613, 15621, 15631, 15641, 15653, 15661, 15673, 15681, 15691, 15701, 15713, 15721, 15731, 15741, 15753, 15761, 15773, 15781, 15791, 15801, 15813, 15821, 15831, 15841, 15853, 15861, 15873, 15881, 15891, 15901, 15913, 15921, 15931, 15941, 15953, 15961, 15973, 15981, 15991, 16001, 16013, 16021, 16031, 16041, 16053, 16061, 16073, 16081, 16091, 16101, 16113, 16121, 16131, 16141, 16153, 161

Chcemy pokazać, że jeśli $n \neq P$, to alg. zwróci żart.

Jak mogłyby się powinny? Na pewno nie w liście 6.

Czyli tym razem w 6.

Treba pokazać, że nie ma ~~spójnych~~ możliwości aby dodać

do liścia 6 dla $\langle n \neq P \rangle$.

Fakt 2

mocne na ciąkach

Istnieje $r \leq \max(3, \lceil \log^5 n \rceil)$ t.ż. $\sigma_r(n) > \log^2 n$.

D-d

Dla $n=2$ i $\max r=3$ jest OK.

Założymy $n > 2$. Wtedy $\lceil \log^5 n \rceil \geq 10$. Niech $B = \lceil \log^5 n \rceil$

Niech r to największa liczba, która

nie jest dzielnikiem all założenia $\rightarrow r \leq B$

$$\frac{n^{\lceil \log B \rceil}}{n} \cdot \prod_{i=1}^r (n^i - 1)$$

Niech $r = p_1^{d_1} p_2^{d_2} \dots p_k^{d_k}$. Jeżeli $p_i \mid n$, to $p_i^{d_i} \mid n^{d_i} \mid n^{\lceil \log B \rceil}$,

bo musi być $d_i \leq \log B$. Zatem jest pewne $p_j \nmid p_i$ $\forall i \neq j$ i takim.

i $p_j \nmid n$. Zatem $\frac{r}{(r, n)}$ też nie działa obyczaj.

Czyli $r \nmid n$.

Porządku $r \nmid n^i - 1$, czyli $n^i \not\equiv 1 \pmod r$ dla $i \leq \lceil \log B \rceil$.

Czyli $\sigma_r(n) > \log^2 n$. Czyli r jest OK. Treba jeszcze juzure,

$\lceil \log \cdot \text{Twierdza} \rceil = 2$ więc $r \leq \lceil \log^5 n \rceil = B$.

Fakt: Dla $m \geq 7$ $\text{LCM}(1, 2, \dots, m) \geq 2^m$. (pot strony dwukrotnie)

Many

$$n^{\lfloor \log_2 B \rfloor} \cdot \prod_{i=1}^{\lfloor \log_2 n \rfloor} (n-i) \leq n^{\lfloor \log_2 B \rfloor + \frac{1}{2} \log_2 (\log_2 n - 1)} \leq n^{\log_2 n} = 2^{\log_2 n} \leq 2^B$$

Trudność obliczenia $\text{LCM}(1, \dots, B)$ jest $\Omega(n^{\log_2 B})$.

Skoro $B \geq 10 > 2$, to $\text{LCM}(1, \dots, B) \geq 2^B$. Wszystko $\in P$.

$\boxed{\text{dowód}}$ nie ilorazem. Czyli $v \leq B$. OK.

\square Skonczone

Zobaczmy, że to implikuje, że alg. jest w PTIME.

$\boxed{\text{cw}}$

Krok 1 - charakteryzacja.

Krok 2 - spr. mocy lesszej niż $\log_2 n$, kiedy $\log_2 n$ kwotą.

Krok 3 - NWD jest szczególnie.

Krok 4 - jasne

$\boxed{\text{cw}}$

Krok 5 - trzeba pokazać dla danego v jest to szczególnie.

Przykłady. Wszystkie liczby leżące pomiędzy $\log_2 v$ i $\log_2 (v+1)$ (tzn. rozbite na dwie części) są podzielne przez v (czyli co najmniej dwa). To prosty szczególnie potęgowań.

Krok 6 - jasne

Dowód

Przedstawimy do trudniejszej części. Zauważmy, że dającą d6, chcemy, by

$\text{Pomocnicza}(v, p) > 1$, to istnieje $p \in P$, $p \mid v$ i $\text{Pomocnicza}(p) > 1$.

Many $\nexists p \mid v$, bo przeszedł krok 3 (a mówiąc o 6).

Ustalimy na cały czas $p, v \in \mathbb{N}$. Oznamy $d = \lfloor \sqrt{v/p} \rfloor \cdot \log_2 v$.

$\text{Pomocnicza}(v, p) \leq \frac{v}{dp} \leq \frac{v}{\lfloor \sqrt{v/p} \rfloor \cdot \log_2 v} \leq \frac{v}{\sqrt{v/p} \cdot \log_2 v} = \frac{\sqrt{v/p}}{\log_2 v} = \frac{\sqrt{p}}{\sqrt{v} \cdot \log_2 v} = \frac{1}{\sqrt{v} \cdot \log_2 v} \cdot \sqrt{p} \leq \frac{1}{\sqrt{v} \cdot \log_2 v} \cdot \sqrt{v+1} \leq \frac{1}{\sqrt{v} \cdot \log_2 v} \cdot \sqrt{2v} = \frac{1}{\sqrt{v} \cdot \log_2 v} \cdot \sqrt{2} \cdot \sqrt{v} = \frac{\sqrt{2}}{\log_2 v} < 1$

Many $(x+a)^n = x^n + a \pmod{x^r-1, p}$

dla $0 \leq a \leq l$.

w szczególności też

$$(x+ca)^n = x^n + ca \pmod{x^r-1, p} \quad (1)$$

dla $0 \leq a \leq l$.

Drukże Lemma 1 many

$$(x+ca)^p = x^p + ca \pmod{x^r-1, p} \quad (2)$$

dla $0 \leq a \leq l$.

Fakt 3

Z tego wynika, że dla każdego a ,

$$(x+ca)^{\frac{p}{r}} = x^{\frac{p}{r}} + ca \pmod{x^r-1, p} \quad (3)$$

dla $0 \leq a \leq l$.

D-d

Not f $\in F_p[x]$ dla $p \neq r$. Wtedy z MTF wynika, że

$$f(x^p) = [f(x)]^p$$

Many wyciągnąć z $(x+ca)^{\frac{p}{r}}$ i z $(x+ca)^p$

$$(x^{\frac{p}{r}} + ca)^p = (x^{p \cdot \frac{n}{r}} + ca) = x^n + ca = (x+ca)^n = (x+ca)^{p \cdot \frac{n}{r}} \pmod{x^r-1, p}$$

(1)
fakty pow.
czytaj top
nie trzeba

Many

$$f = x^{\frac{p}{r}} + ca, g = (x+ca)^{\frac{n}{r}} \quad \text{Many } f^p = g^p, \text{ chyba } f = g.$$

$$(f-g)^p = f^p - g^p \pmod{p}, \text{ ale } (f-g)^p = 0 \in F_p[x]/x^r-1$$

To wydaje się nieco dziwne, ale może da się zrobić

D

(z dla dow) $\alpha^m \equiv (\alpha \mod p)^m$

Def. 1 Mówimy, że fud. $f(x)$ do kierka mew N jest intr. (innych) dla x , jeśli dla $a \in \mathbb{Z}_p$ istnieje $b \in \mathbb{Z}_p$ takie, że $f(a) = f(b) \pmod{x^{p^N}-1, p}$

$$(1) f(x^m) \equiv f(x^n) \pmod{x^{p^N}-1, p}$$

Czyli np. $n, p, \frac{n}{p}$ są intr. dla $(x+a)$ dla

$$(2) (a \geq 0, 0 \leq a \leq p-1) \quad \alpha^m \equiv (\alpha + a)^n \pmod{x^{p^N}-1, p}$$

Fakt 4

Jesli m, k są intr. dla $f(x)$, to $m \cdot k$ też jest intr.

$$(3) \text{D-d} \quad (a^m \equiv b^m \pmod{x^{p^N}-1, p}) \quad \alpha^m \equiv (\alpha^k)^m \pmod{x^{p^N}-1, p}$$

Ponieważ k jest intr., to

$$f(x^m) = f(x^k)^m \pmod{x^{p^N}-1, p}$$

$$f(x^k)^m = f(x^{km}) \pmod{x^{p^N}-1, p}$$

$$= f(x^{km}) \pmod{x^{p^N}-1, p}, \text{ bo } x^{p^N-1} \mid x^{km} - 1$$

$$(a^m \equiv b^m \pmod{x^{p^N}-1, p}) \Rightarrow f(a^m) \equiv f(b^m) \pmod{x^{p^N}-1, p}$$

Podobnie

Fakt 5

Jesli m jest intr. dla $f(x)$ i $g(x)$, to dla $f(x) \cdot g(x)$ też

D-d

$$[f(x) \cdot g(x)]^m = f(x)^m \cdot g(x)^m = f(x^m) \cdot g(x^m) \pmod{x^{p^N}-1, p}$$

W związku z tym każda liczba $\lambda \in \mathbb{Z}_p$ ze zbioru $I = \left\{ \left(\frac{n}{p}\right)^0 p^j \mid j \geq 0 \right\}$
 jest inspektorowa dla każdego ułamka ze zbioru $P = \left\{ \prod_{n=0}^{\infty} (x+n)^\lambda \mid \lambda \in I \right\}$.

Nabór tych edefiniujących dukt grupy, które będą sufficjalne kluczowe w dowodzie.

Miejsce pierwsza grupa dla G to zbiór reszt kresów λ modulo n .

To podgrupa Z_r^* , bo $n \perp r$, $p \perp r$. Miejsce $|G| = t$.

G jest generowana przez $n^0 p$ nad r , ponieważ $O_r(n) > \log^2 n$,
 to też $t > \log^2 n$.

Teraz przechodzimy do dalszej grupy. Miejsce $Q_r(x)$ to

r -ty res. cyklotomowy nad F_p . $Q_r(x) \mid x^{r-1}$ (bo to tylko niektóre pierwiastki).

Opisac tez

Fakt 6 [LN86 - Intro to finite fields and their appl.]

$Q_r(x)$ posiada reszta na \mathbb{Z}_p niezdzielnego cyklu rzędu $O_r(p)$

(zobacz, co $\deg Q_r(x) = \varphi(r)$, czyli $O_r(p) \neq \varphi(r) = \deg Q_r(x)$)

Miejsce $h(x)$. Ileśne jednym z takich cyklieków

Ale powiedzmy $O_r(p) > 1$, to $\deg h(x) > 1$.

Drużą grupą to G . To są wszystkie reszty ułamków z P

modulo $h(x)/p$. Grupa G jest generowana przez

$x, x+1, \dots, x+l$ nad $h(x)/p$ (czyli w ciele $F_p[x]/h(x)$).

Ciąg wzorów dla $a \rightarrow b$ dla b oznacza

$a \circ b = b$ dla $a, b \in \mathbb{R}$

Rozważ dowód do 3. lematu pokazywac, że:

$$- |G| \geq \binom{t+r}{t-1} \quad (\text{lemat 2})$$

$$- |G| \leq n^{\sqrt{r}} \quad \text{o ile } n \text{ nie jest potęgą } p \quad (\text{lemat 3})$$

$$- \binom{t+r}{t-1} > n^{\sqrt{r}} \quad (\text{lemat 4})$$

Czyli n to potęga p , czyli $n=p^k$, czyli $n \in P$.

Dla tego to taka idea - nie mamy pewności to jasno techniczne problemy dotyczące tego.

Lemat 2

$$|G| \geq \binom{t+r}{t-1}$$

Ależ tak!

Jednak pewnie jest jakieś idea dla tego
najmniejszej $|G|$.

D-d

$$\text{Nied } F = F_p[x]/h(x)$$

Wtedy, jeśli $h(x) \mid Q_r(x) \mid X^r - 1$, wtedy $X^r = 1 \pmod{h(x)}$, wtedy
 $X^r = 1 \in F$.



Zawsze powodzie $X^k \neq 1 \in F$ dla $k < r$.

Pokazemy teraz, że każde dwa (wielomiany) stopnia $\leq t$ z P

małyż się na reszcie reszty w F . Potem pokażemy, że jest ich
co najmniej $\binom{t+r}{t-1}$.

Zauważmy, że $f(x) = g(x) \in F$. Nied $m \in I$.

Mamy $f(x^m) = g(x^m) \in F$. Zatem x^m to pierwiastek

$Q(y) = f(y) - g(y)$ dla każdego $y \in I$. Ponieważ $m < r$ (to podał podany w I),

to X^m jest pierwiastkiem z jedynki st. Wielomianu r .

A więc jest co najmniej $|G| - f$ różnych pierwiastków z 1 st. wielomianu r .

Ależ tak! Jednak st. $Q \leq t$ i tego ja wykazuję dla $f \neq g$.

Sp. n. i zat. że $f = g \in F$.

(stąd, iż $x^i \neq x^j$, czyli $h + x^{i-j}$)

Twarz polecamy ile jąt tablicz wad. (przyjmajemy).

Mamy $\ell = \lfloor \sqrt{q(r)} \log n \rfloor < \sqrt{r} \log n < r$ oraz $p \geq r$ (krok 3 i w. b.)

Zatem dla $(i'_1 + j) \leq \ell$ mamy $i'_1 + j \in F_p$.

Zatem $X, X+1, \dots, X+\ell$ są reszty F_p . Ponieważ $\deg h(x) \geq 1$, to

$X+a \neq 0$ dla $0 \leq a \leq \ell$. A więc jest min. $\ell+1$ różnych
wad. st. 1. Doby mied ~~st. 2~~ st. 3B stąd to
 $t-1$ różnych wad. w $\ell+2$ mocy.

Bierzemy $\ell+1$ różnych wad. wstawiamy w $t-1$ różnych.

Notatka: trzeba wybrać $t-1$ różnych z $t-1 + \ell + 1$ różnych, wykorzystując

~~(t+ℓ)~~ $\binom{t+ℓ}{t-1}$.

□

Lemat 3

Jeśli n nie jest potęgą p , to $|G| \leq n^{\sqrt{r}}$.

D-d

Rozważmy $\hat{I} = \left\{ \left(\frac{n}{p}\right)^i \cdot p^j \mid 0 \leq i, j \leq \lfloor \sqrt{r} \rfloor \right\} \subseteq I$

Jeśli n nie jest potęgą p , to \hat{I} ma $\left(\lfloor \sqrt{r} \rfloor + 1\right)^2 > t$

różnych elementów. Ponieważ $|I| = t$ to wśród nich jest co najmniej 2 z \hat{I}
modulo r , to pierwsze dwoje liczb z \hat{I} muszą być równie równe.

Niech będzie to m_1, m_2 , $m_1 > m_2$. Wtedy

$$\cancel{x^{m_1}} = \cancel{x^{m_2}} \pmod{p}$$

$$x^{m_1} = x^{m_2} \pmod{p}$$

Mamy $\deg f(x) \in P$. Wtedy

$$f(x)^{m_1} = f(x^{m_1}) = f(x^{m_2}) = f(x)^{m_2} \pmod{x^{r-1}, p}$$

Zatím $f(x)^{m_2} = f(x)^{n_2} \in F$.

A když $f(x) \in G$ ještě primitivní nebo nám

$Q'(Y) = Y^{m_2} - Y^{n_2} \in F$. Skoro $f(x)$ je doslovy element g ,

to $\deg Q' \geq |g|$.

Jednak $\deg Q' = m_2 \leq \left(\frac{n}{p} \cdot p\right)^{\lfloor Lv_F \rfloor} = n^{\lfloor Lv_F \rfloor}$.

Zatím $|g| \leq n^{\lfloor Lv_F \rfloor}$

Lemat 4

$$\binom{t+l}{t+1} > n^{V_F}$$

$$t \leq \sqrt{v_F} \\ t > \log_2 n \\ l = \lfloor V_F \log_2 n \rfloor$$

D-d

$$\text{dop} \quad \binom{t+l}{t+1} \geq \binom{LV_F \log_2 n + 1 + l}{LV_F \log_2 n + 1 - 1}$$

$$\binom{2^{n+1}}{n} > 2^n$$

$$t < \binom{t+1}{t+1} \geq \binom{2^{LV_F \log_2 n} + 1}{2^{LV_F \log_2 n}}$$

I = $\sum_{i=0}^{2^{n+1}-1} \binom{i}{n} = 1, \quad \binom{2^{n+1}}{2^{n+1}}$

$$\binom{x}{a} > \binom{y}{a}$$

$$\lfloor V_F \log_2 n \rfloor > \lfloor \log_2 n \rfloor \geq 1,$$

Me x/y

$$+ \text{remake ratio. dla } \binom{2^{n+1}}{n} > 2^n$$

$$> \sqrt{V_F} \cdot 2^{V_F \log_2 n} = n^{V_F}$$

W

zjistit výsledek

$$(q, \infty) \times (\infty, \infty)$$

$$\binom{q}{x} = \binom{q}{x} + \binom{q}{x} = \binom{q}{x} = \binom{q}{x}$$