Nombres premiers, codes, tissus

Catherine Goldstein
Institut de mathématiques de Jussieu
CNRS, UPMC

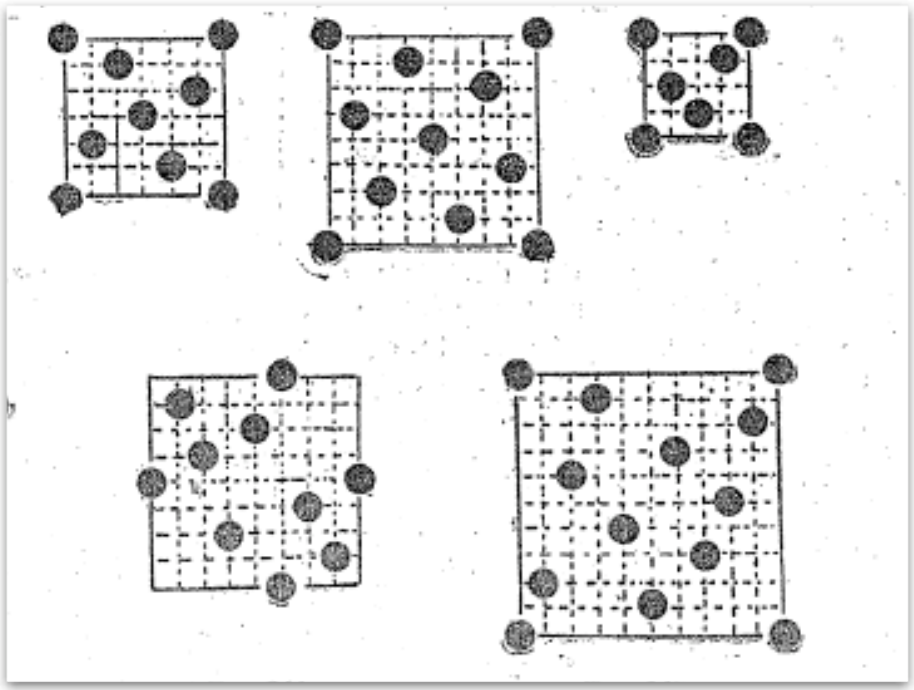
Le tissu de mensonges…

Max Ernst (1959)

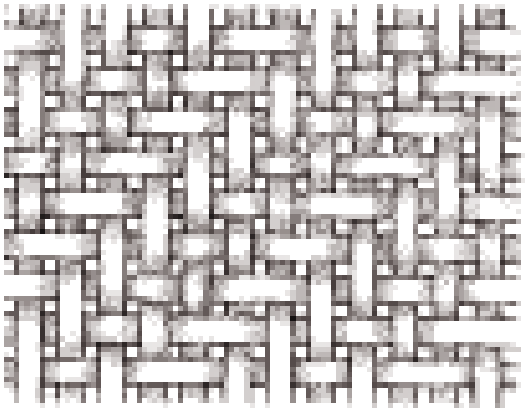
(C) ADAGP — Photo CNAC/MNAM, Dist. RMN / Jean-Claude Planchet

cf. site Réunion des musées nationaux
http://www.photo.rmn.fr/cf/htm/CSearchZ.aspx?o=&Total=1&FP=4060970&E=2K1KTSYGUV2J&SID=2K1KTSYGUV2J&New=T&Pic=1&SubE=2C6NU0VCT3CG

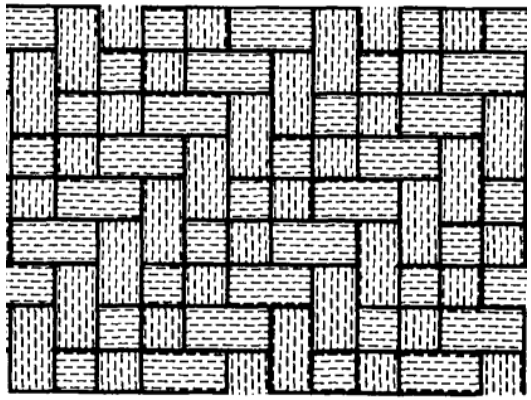
Extrait du journal « L'INDUSTRIE TEXTILE »



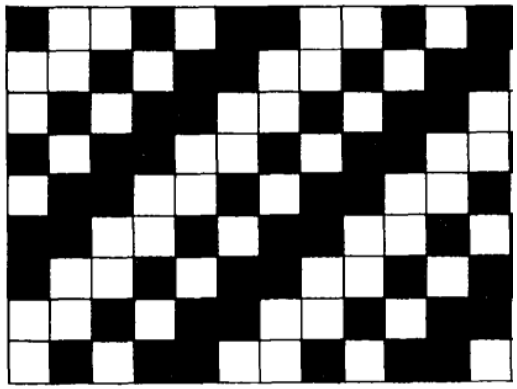
Des tissus de vérités …
L'arithmologie textile



a



b

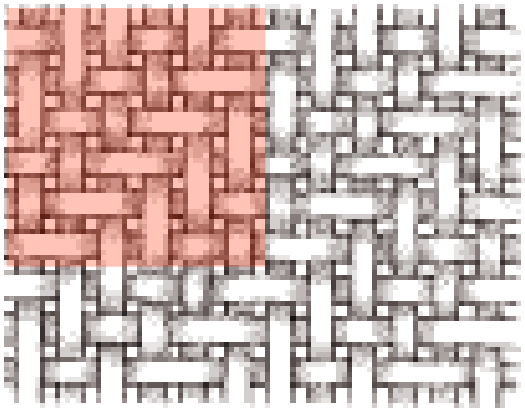


c

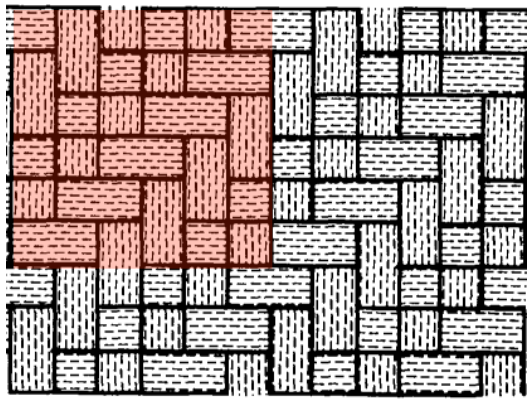
(a) tissu (presque) réel (b) tissu idéalisé (c) dessin ou diagramme associé à une armure sergé (twill) de 6

d'après B. Grunbaum et G. Shephard, *Mathematics Magazine* 53/3, 1980

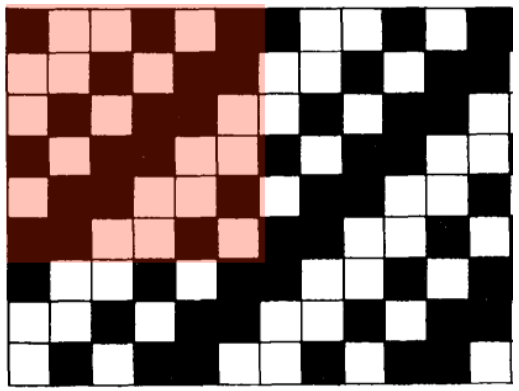
Armure = mode d'entrecroisement des fils de chaîne et des fils de trame.
Rapport d'armure = surface minimum nécessaire pour voir la loi de répétition des fils



a



b



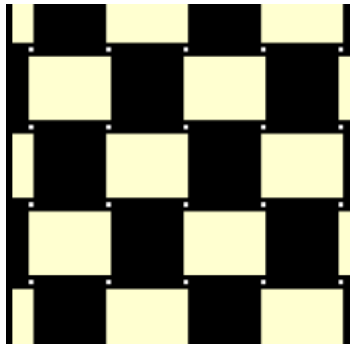
c

(a) tissu (presque) réel (b) tissu idéalisé (c) dessin ou diagramme associé à une armure sergé (twill) de 6

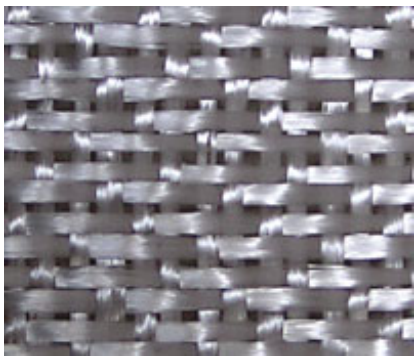
d'après B. Grunbaum et G. Shephard, *Mathematics Magazine* 53/3, 1980

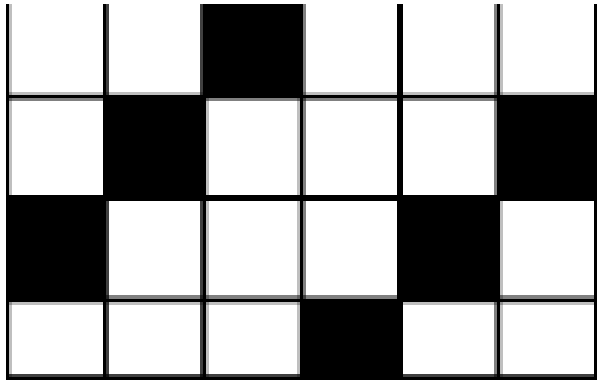
Armure = mode d'entrecroisement des fils de chaîne et des fils de trame.
Rapport d'armure = surface minimum n x n nécessaire pour voir la loi de répétition des fils

Armures des tissus



Armure toile
(module 2)





Armure sergé
(module 4)

Armure satin (régulier)

- 1 point de liage sur 1 trame et 1 chaîne dans le rapport d'armure
- décochement a tel que le point de liage de la colonne k soit à la ligne ka (au module p près)
- le tissu "tient" si a et p sont premiers entre eux
- a=1 ou p-1 => sergé !
- ex: pas de satin régulier de module 6

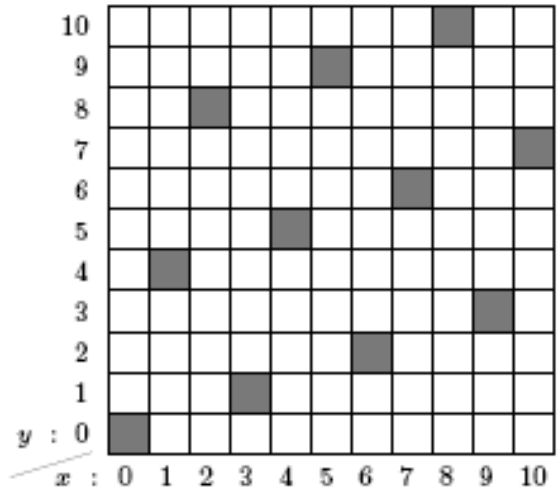


Figure 1. Satin de module 11 et de décochement 4

(d'après A. M. Décaillot, RHM 2002)

"Il serait utile [...] d'avoir des procédés rationnels, des formules faciles à retenir, qui permissent d'exécuter, sans hésitation ni perte de temps, la mise en carte du satin proposé. La plupart du temps, lorsque l'on a de semblables dispositions de satins à écrire, on procède par de longs tâtonnements". (Édouard Gand, *Bulletin de la Société industrielle d'Amiens,* 1867)

=> **Edouard Lucas** c. 1870-1880: Arithmétique des restes mod n (arithmétique modulaire, des résidus, des congruences…) appliquée aux problèmes textiles

Edouard Lucas (1842-1891)

Arithmétique modulaire et satins

- Classer les satins réguliers (de module p premier) : le (petit) théorème de Fermat.
- Trouver les satins carrés, qui sont ceux tels que si a' est associé à a (i.e. : p divise aa'-1), alors a=p-a'

Arithmétique modulaire et satins

- Classer les satins réguliers (de module n) : le (petit) théorème de Fermat.

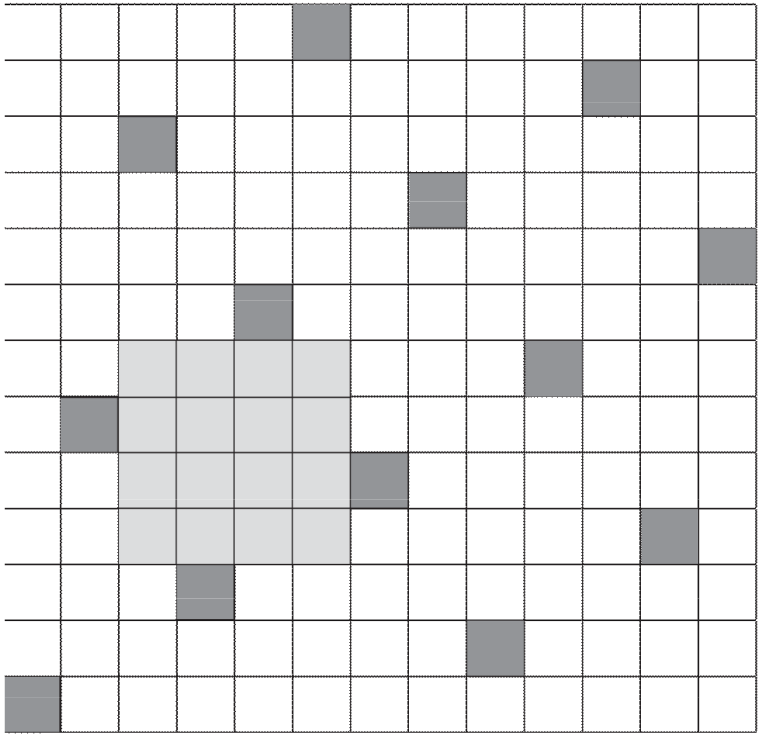
Si a et n premiers entre eux, le plus petit g tel que n divise $a^g - 1$ divise $\varphi(n)$ (nombre d'entiers <n et premiers à n)

Arithmétique modulaire et satins

- Trouver les satins carrés : si a' est associé à a (i.e. : p divise aa'-1), alors a=p-a'

Théorème : Soit p impair. Il existe un satin carré régulier de module p ssi p est de la forme x^2+y^2, donc ssi p de la forme 4n+1

"On doit considérer les armures …satins carrés …comme la fidèle représentation géométrique des racines des congruences $x^2+1=0$ mod p"



Satin carré de module 13 et
de décochement 5

Retour à la théorie

Carl Friedrich Gauss
(1777-1855)

- "Une des meilleures têtes mathématiques de l'Europe" (Poinsot, 1807)
- contributions fondamentales en théorie des nombres, analyse, géométrie différentielle, astronomie, géodésique,…
- 1801: *Disquisitiones arithmeticae* et prédiction de l'emplacement de Cérès

Recherches arithmétiques

- Vos Disquisitiones vous ont mis tout de suite au rang des plus grands géométres (Lagrange, 1804)

- Mr Gauss a traité d'une manière entièrement nouvelle toute cette théorie [des nombres] dans un ouvrage singulièrement remarquable dont il nous est impossible de donner une idée parce que tout y est nouveau, jusqu'au langage et à la notation (Ac. des sciences à Napoléon)

SCIENCES.

ANTIQUITÉS CELTIQUES

DISQVISITIONES

ARITHMETICAE

AVCTORE

D. CAROLO FRIDERICO GAVSS

LIPSIAE

IN COMMISSIS APVD GERH. FLEISCHER, Jun.

1801.

- Congruences
- Formes quadratiques
- Application I: factorisation
- Application II: inscription d'un polygone régulier dans un cercle

Congruences

- Si n divise a-b, on dit que a et b sont congrus modulo n, on écrit $a \equiv b \pmod{n}$
- congruences  égalités
- étude des puissances $1, a, a^2, a^3, a^4, \ldots$ d'un entier modulo n, $(a, n) = 1$ (petit th. de Fermat, racines primitives)
- étude des équations aux congruences ; théorème fondamental dans le cas quadratique (loi de réciprocité)

Formes quadratiques

Exemples : x^2+y^2, $3x^2+10xy+y^2$

En général : $ax^2+2bxy+cy^2$, avec a, b, c entiers

- Question 1: quels nombres sont représentés par une forme donnée ? Est-ce que 21 est somme de deux carrés ? Est-ce que 60n+11 divise$3x^2-5y^2$?
- Question 2 : classer les formes à changement de variables (inversible) près

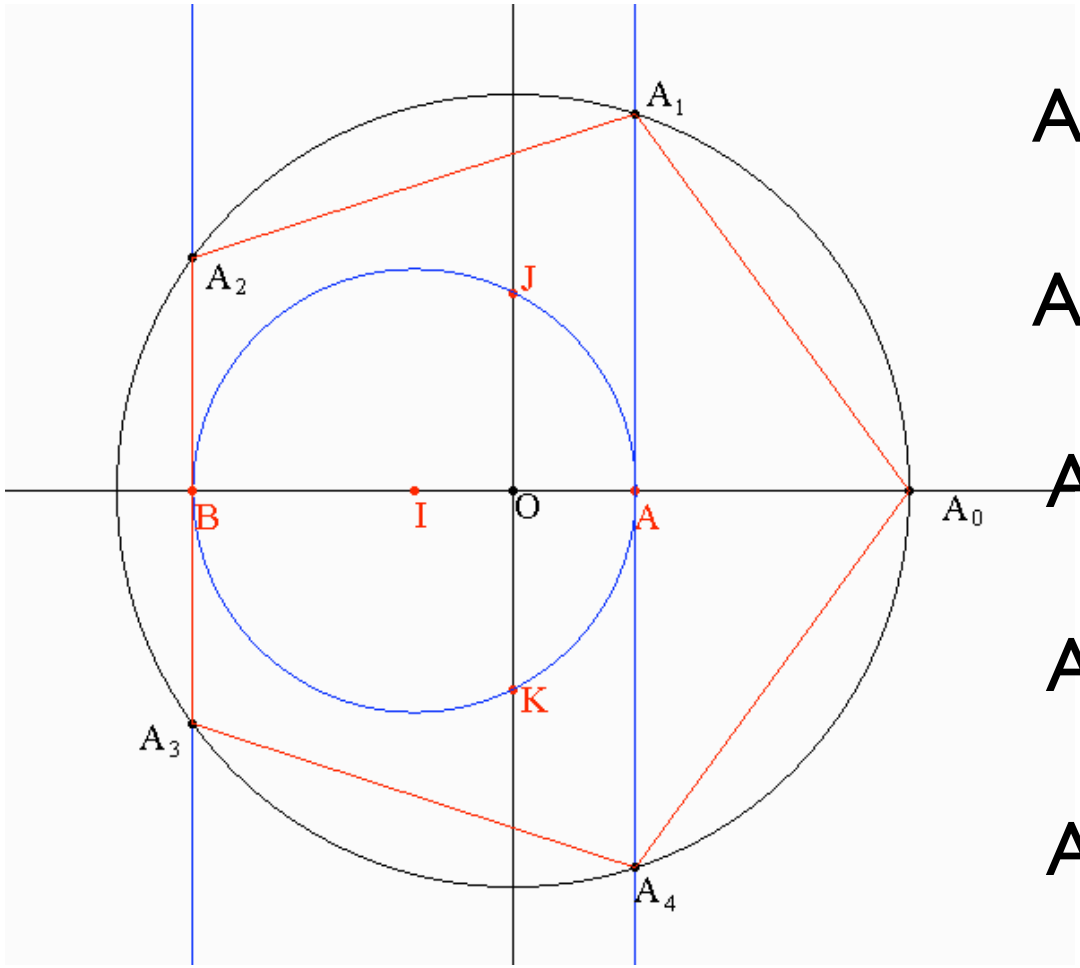
$x=ux'+vy'$, $y=u'x'+v'y'$, avec u, u', v, v' entiers et $uv'-u'v=\pm 1$

Notion d'*invariant*, le déterminant b^2-ac;
nombre de classes de déterminant fixé ;
bons *représentants* de chaque classe,
composition de formes , etc.

Polygone régulier inscriptible dans un cercle

- Dès l'Antiquité, triangle, carré, pentagone inscrits dans un cercle *à la règle et au compas*.
- Gauss donne des conditions sur le nombre de côtés n pour que cette inscription soit possible : si n premier, $n-1 = 2^m$ (et $m=2^k$), donc n est un nombre de Fermat (3, 5, 17, 257, 65537), en général produit de 2^m et de premier $2^{m'}+1$
- Utilise sa théorie des congruences pour recoder les points

Polygone régulier inscriptible dans un cercle



A_0 point (1,0)

A_1 point (cos 2π/5, sin2π/5)

A_2 point (cos 4π/5, sin4π/5)

A_3 point (cos 6π/5, sin6π/5)

A_4 point (cos 8π/5, sin8π/5)

http://les-mathematiques.u-strasbg.fr/phorum/read.php?f=2&i=286850&t=286850

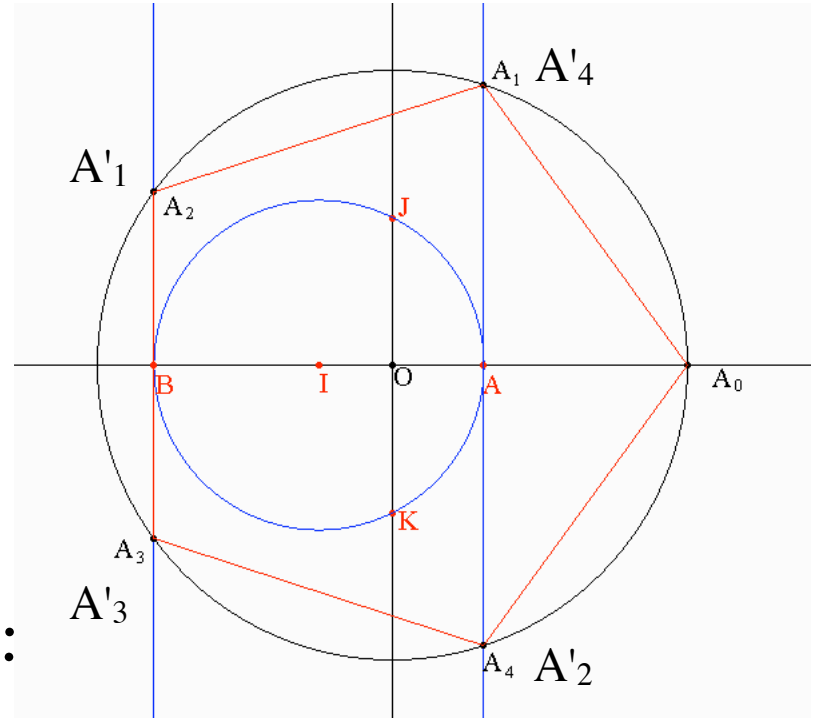
Polygone régulier inscriptible dans un cercle

• Nouveau codage des points à l'aide d'une racine primitive modulo 5 : si $(k, 5)=1$, $k=2^{k'} \bmod 5$.

A_0	(1,0)	$e^{0i\pi/5}$	a^0	a^0	A'_0
A_1	$(\cos 2\pi/5, \sin 2\pi/5)$	$e^{2i\pi/5}$	a^1	a^{24}	A'_4
A_2	$(\cos 4\pi/5, \sin 4\pi/5)$	$e^{4i\pi/5}$	a^2	a^{21}	A'_1
A_3	$(\cos 6\pi/5, \sin 6\pi/5)$	$e^{6i\pi/5}$	a^3	a^{23}	A'_3
A_4	$(\cos 8\pi/5, \sin 8\pi/5)$	$e^{8i\pi/5}$	a^4	a^{22}	A'_2

Polygone régulier inscriptible dans un cercle

- Le nouveau codage incite à regrouper certains points :
  $a^{2^1} \longrightarrow a^{2^3} \longrightarrow a^{2^5} = a^{2^1}$
  $a^{2^2} \longrightarrow a^{2^4} \longrightarrow a^{2^6} = a^{2^2}$



- $a^{2^1} + a^{2^3}$, $a^{2^2} + a^{2^4}$ sont racines d'une équation quadratique, donc constructibles à la règle et au compas:
  $a^{2^2} + a^{2^4} = \cos 2\pi/5 = (\sqrt{5}-1)/4$
- On en déduit tous les sommets Ai

Primalité et factorisation

- **Le problème où l'on se propose de distinguer les nombres premiers des nombres composés et de décomposer ceux-ci en leurs facteurs premiers, est connu comme un des plus importants et des plus utiles de toute l'Arithmétique…Aussi nous ne doutons pas que les deux méthodes suivantes dont nous pouvons affirmer la brièveté et l'efficacité d'après une longue expérience , ne plaisent aux amateurs de l'Arithmétique.** (R. A., art. 329)

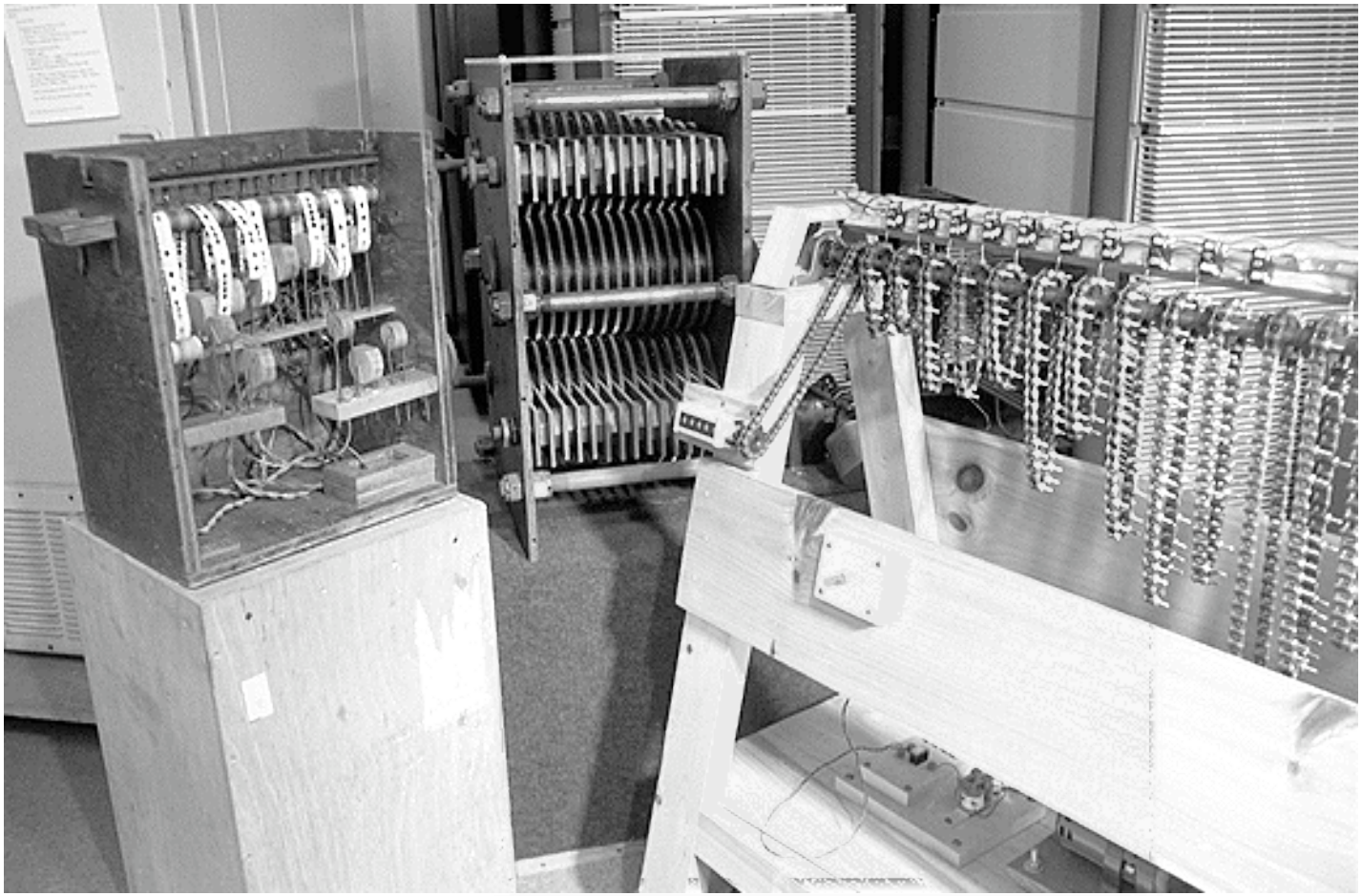
Primalité et factorisation

- **1ère méthode : Principe : si n est un carré x^2 modulo M, c'est un carré modulo m, pour tout m diviseur de M. Donc 1) on liste les restes n_i de carrés mod M, 2) on exclut les m pour lesquels un n_i ne marche pas. Ex. pour M= 997331 : les résidus n_i = -6, 13, -14, 17, 37, -53 excluent m<127 et 997331 = 127 . 7853.**

- **2ème méthode : M comme diviseur de formes quadratiques $x^2 + Dy^2$. Ex : M=4272943 = $x^2 + 286y^2$ (= $(1113)^2 + 286(103)^2$) est premier**

Implémentation

- Exclusion : cribles
- Machines à cribler : baguettes, cellules photo-électriques et chaînes de vélo



Les cribles de D. H. Lehmer (c. 1930)

Computers in Number Theory, Conférence à Oxford, England, 1969 (photo J. B. Cosgrave)

Les *Recherches* aux USA

- D. N. Lehmer (1867-1938), D. H. Lehmer (1905-1991), E. Lehmer (1906-2007), R. Robinson (1911-1994), D. Shanks (1917-1996), …
- Carnegie Institution, ENIAC, SWAC, Institute for Numerical Analysis (UCLA) (cf. L. Corry, Hunting Prime Numbers…)

D. H. Lehmer (suite)

- Thèse de D. H. Lehmer: *An extended Theory of Lucas's function*
- "The most compelling urge to the study of mathematics is not its practical application to the study of every day, bread-and-butter life, but lies in the romance and glamour surrounding its mysterious secrets" (D. H. Lehmer, 1932, d'après L. Corry, *Hunting primes…*, 2008)

Test de primalité de Lucas-Lehmer I

- Suite (u_n, v_n) de Lucas. Soient a et b deux entiers, $(a,b)=1$. On pose $u_0=0$, $u_1=1$, $u_{n+2}=au_{n+1}+bu_n$ (ou $v_0=2$, $v_1=a$, $v_{n+2}=av_{n+1}+bv_n$)
- Exemples : Nombres de Mersenne: $2^n-1=u_n(3,-2)$, nombres de Fermat $2^{2^k}+1=v_{2^k}(3,-2)$, nombres $s_k=v_{2^k}(1,1)$

Test de primalité de Lucas-Lehmer 1

- Théorème : Si p est de la forme 10k+3 ou 10k-3, et p divise u_{p+1}, mais pas u_d, $d \leq p$ et $d | p+1$, alors p est premier
- Application (Lucas, 1876) $M^{127}=2^{127}-1$ est premier

Test de primalité de Lucas(-Lehmer) II

- Réciproque du théorème de Fermat : Si N impair, il existe a tel que N divise $a^{N-1}-1$ et N ne divise pas $a^{(N-1)/p}-1$ pour p divisant N-1, alors N est premier
- test pratique (mais 37.73 divise $2^{37.73-1}-1$)

Grands nombres premiers

- $2^{43\,112\,609}-1$, avec 12 978 189 chiffres, découvert le 23 août 2008 à UCLA par Edson Smith, George Woltman, Scott Kurowski, et al., dans le cadre du projet GIMPS

316, 470,269,330,255,923,143,453,723,949,
337,516,054,106,188,475,264,644,140,304,176,732,811,247,493,069,368,692,043,
185,121,611,837,856,726,816,539,985,465,097,356,123,432,645,179,673,853,590,
577,238,179,357,900,876,426,103,943,782,376,494,591,742,934,588,497,117,587,
146,916,972,984,761,159,060,873,250,939,462,085,575,740,754,577,098,620,558,
011,779,529,884,042,198,287,643,319,330,465,064,455,234,988,142,139,565,785,
447,474,023,546,353,758,537,324,801,838,120,387,600,868,416,525,400,790,381,
285,888,256,687,085,855,456,231,577,527,939,305,920,811,766,585,308,670,132,
129,155,221,804,381,548,625,787,943,020,694,528,015,999,221,718,191,557,761,
789,038,539,522,349,746,808,797,476,907,664,050,601,248,473,206,874,133,194,
663,585,334,983,805,734,803,620,705,778,270,910,561,716,767,680,954,814,415,
310,034,502,440,445,161,332,363,611,749,326,163,346,444,542,332,941,724,120,
365,148,892,204,420,675,302,563,534,393,044,688,859,445,173,161,934,549,310,
336,116,821,178,855,375,531,041,423,821,706,430,796,012,246,288,037,483,476,
218,396,982,916,073,816,451,058,991,831,512,686,327,488,459,585,043,246,778,
160,788,873,343,661,684,676,258,006,436,582,840,222,063,757,785,048,077,389,
404,912,747,062,648,672,186,003,349,751,782,781,879,120,470,020,388,873,779,
589,349,589,877,119,954,283,343,288,199,886,936,593,732,250,320,339,998,...
.....
859,186,062,158,287,951,177,386,802,987,626,023,010,652,739,182,295,541,392,
918,020,056,838,360,135,679,872,860,483,416,916,652,487,086,962,757,779,741,
806,708,471,114,811,595,228,196,181,682,379,446,066,996,833,600,335,035,579,
534,312,511,612,725,344,467,160,112,063,722,352,068,121,255,162,528,031,252,
563,906,005,692,627,824,649,052,422,502,206,934,159,709,803,688,308,998,372,
051,463,441,115,976,028,226,909,156,682,192,013,981,830,822,014,104,610,660,
911,290,342,036,586,081,253,355,079,240,744,261,814,870,918,055,920,432,372,
301,962,016,835,359,462,310,980,067,434,984,625,380,787,247,802,532,758,511,
333,502,460,778,884,339,034,019,700,927,663,958,167,698,908,010,736,101,410,
136,996,852,925,703,272,553,544,622,464,685,928,707,526,568,105,993,689,915,
218,073,801,443,404,945,008,266,425,932,413,139,826,915,084,069,991,159,279,
791,908,398,130,223,304,824,083,119,093,195,998,014,562,456,347,941,202,195,
900,928,079,670,729,447,921,616,491,887,478,265,780,022,181,166,697,152,511

Sécurité, cryptographie, cryptanalyse

- La cryptographie à clé publique ou asymétrique repose sur des *fonctions à sens unique (fonction trappe)*
- F*onction trappe* : facile à appliquer, difficile de retrouver la valeur initiale
- Exemples : multiplier/factoriser, puissance mod n/logarithme discret

Algorithme RSA

- R(ivest)S(hamir)A(dleman), utilisé sur Internet, cartes bancaires, …)
- Fonction trappe via arithmétique modulaire
- Le module de chiffrement est n=pq, pet q premiers, l'exposant de chiffrement e, (premier à φ(n)=(p-1)(q-1))
- chiffrement: M—>M^e mod n
- déchiffrement : il "faut" avoir d, ed=1 mod φ(n)

Déchiffrer le log discret...: Algorithme " Baby Step Giant Step"

(d'après *Handbook of Applied Cryptography* et M. Bullynck, Mathematical Tables…)

- Origine : Daniel Shanks (CLASNO)… et la section V des *Recherches arithmétiques* de Gauss !
- Question : G groupe cyclique = <a> à n éléments et x dans G, donc $x=a^g$. Calculer g.
- (1): Soit $m=E(\sqrt{n})$, on liste (j, a^j) pour $0 \leq j \leq m$ et on ordonne selon la 2e composante
- (2) Si x listé, ok, sinon, on teste $x(a^{-m})$, $x(a^{-m})^2$, …
- ordre de grandeur : $C\sqrt{n}$ multiplication dans G

Un exemple...:
Algorithme " Baby Step Giant Step"

- Exemple : G restes modulo 113 = <3> à 113 éléments et x=57 dans G, donc $x=3^g$. Calculer g.
- (1): Soit m=11 , on liste (j, 3^j) pour $0 \leq j \leq 11$ et on ordonne selon la 2e composante
- $(a^{-11}) = 38^{11}$ mod 113 = 58 mod 113
- (2)On teste 57(58) mod 113, $57(58)^2$ mod 113, …
- On trouve $57(58)^9$ mod 113 = 3 mod 113
- Donc $57=3^{100}$ mod 113

Pour conclure…

- Dynamique entre applications et théories : pas à sens unique !
- Longue durée des mathématiques
- Modernité : pas seulement les structures

Références

- M. Bullynck, Mathematical Tables and Other Ways to Gauss and Computations, prép. online
- L. Corry, Hunting Prime Numbers from Human to Electronic Computers, The *Rutherford Journal - The New Zealand Journal for the History and Philosophy of Science and Technology*, 2008 (aussi on line)
- A.-M. Décaillot, Géométrie des tissus, mosaïques, échiquiers, mathématiques curieuses et utiles, *Revue d'histoire des mathématiques*, 2002, 8, 145-206
- C. Goldstein, N. Schappacher, J. Schwermer (éds.), *The Shaping of Arithmetic after C.F. Gauss's Disquisitiones,* Springer, 2007
- *Handbook of Applied Cryptography*, online
- A. van der Poorten, A. Stein (éds), *High Primes and Misdemeanours*, AMS, 2004