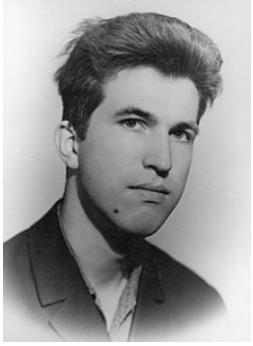
07-04 Histoires de maths

Le crible de Youri Matiassevitch



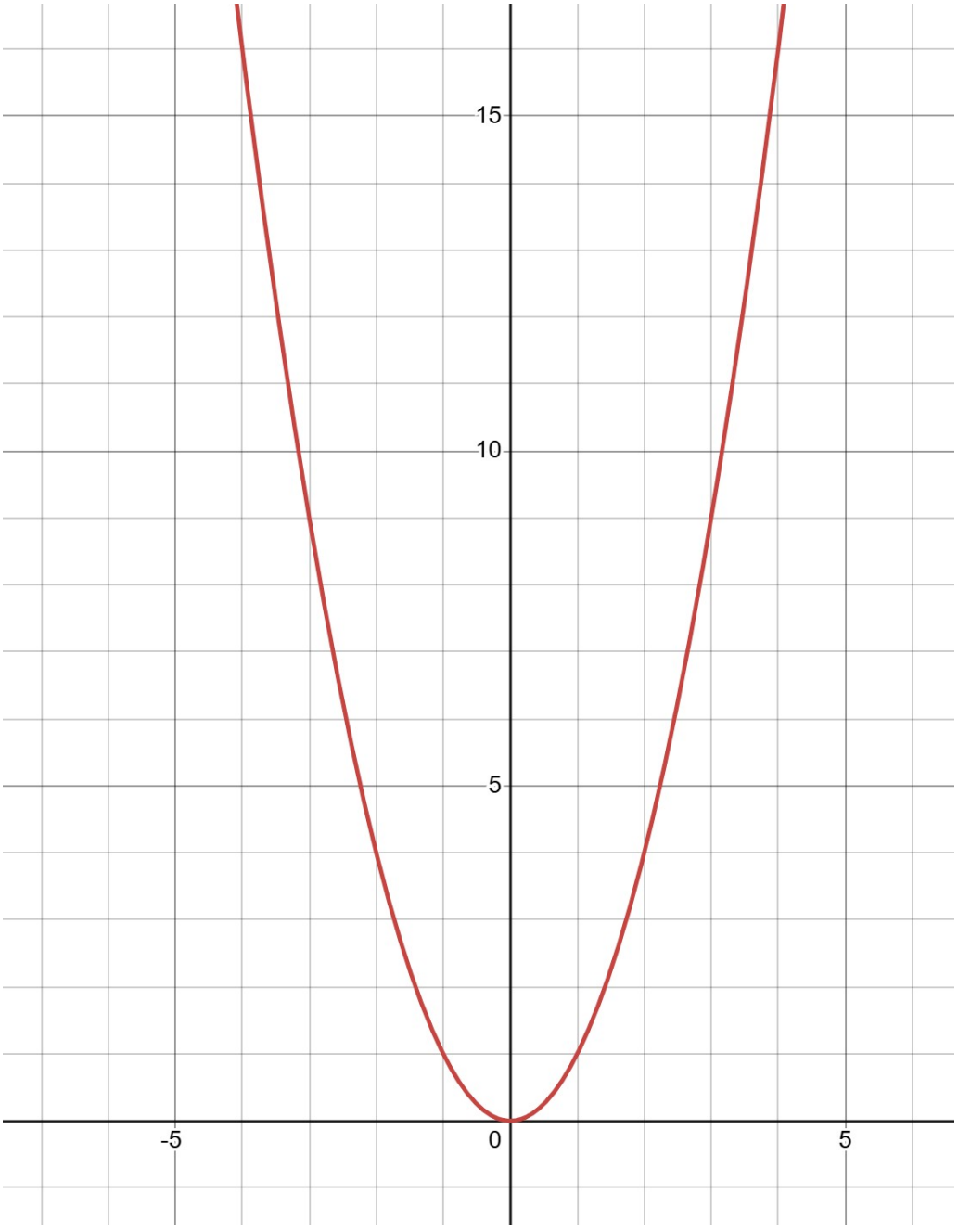
Mathématicien russe, né en 1947. Célèbre pour avoir prouvé, en 1970, l'indécidabilité du dixième problème de Hilbert dont l'énoncé est :

> « On donne une équation diophantienne à un nombre quelconque d'inconnues et à coefficients entiers rationnels. On demande de trouver une méthode par laquelle, au moyen d'un nombre fini d'opérations, on pourra distinguer si l'équation est résoluble en nombres entiers rationnels ».

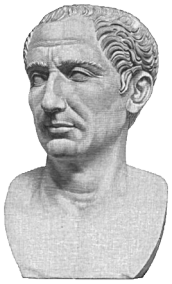
1. Soient a et b deux entiers naturels strictement supérieurs à 1.
On considère la courbe (C) de la fonction carré et les points $A(-a\ ;\ a^2)$ et $B(b\ ;\ b^2)$.
On note $C(0\ ;\ h)$ l'intersection de $[AB]$ avec l'axe des ordonnées.
Placer A, B et C sur le dessin ci-dessous en choisissant des valeurs arbitraires pour a et b.

2. Exprimer h en fonction de a et b.

3. Quelle utilité présente cette activité en ce qui concerne les nombres premiers ?



Le chiffrement RSA

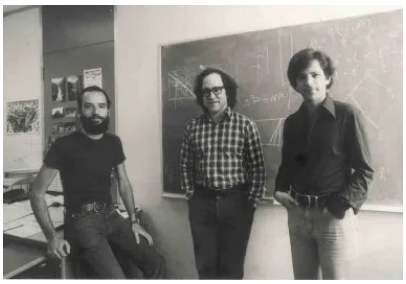


La **cryptologie** est l'union de :

- la **cryptographie** : science du codage.
- la **cryptanalyse** : science du décodage.

Dans ses correspondances militaires, Jules César (-50) décalait chaque lettre de trois rangs dans l'alphabet. Adapté à notre alphabet, l'utilisation de « D » signifiait « A ».

Le chiffrement de César est un **algorithme symétrique** ou **algorithme à clé secrète,** la clé étant l'information permettant de coder et décoder le message.
Un **algorithme asymétrique** repose sur deux clés : une clé publique permettant de coder le message et une clé privée permettant de le décoder.



De gauche à droite sur la photo : Adi Shamir, Ron Rivest et Len Adleman, les inventeurs du système de chiffrement RSA qui fut présenté pour la première fois en août 1977 dans la revue *Scientific American*.

Rivest, Shamir et Adleman souhaitent démontrer que les algorithmes asymétriques possèdent forcément des « failles logiques ».
Ils échouent dans leur projet mais découvrent le système qui porte leur nom.

Soient p et q deux nombres premiers distincts. On pose $N = pq$ et $n = (p-1)(q-1)$.
On choisit un entier c premier avec n. Le couple $(N ; c)$ est la clé publique.
Tout le monde peut la connaître afin de coder de la façon suivante :

« Un entier naturel a est codé en reste b de la division euclidienne de a^c par N ».

Étudions le fonctionnement du chiffrement RSA dans le cas où $p = 5$ et $q = 11$.

1. **a]** Vérifier qu'on a le droit de choisir $c = 3$.
   b] Que devient le nombre 9 une fois codé ?

2. **a]** Résoudre l'équation $3x - 40y = 1$.
   b] En déduire l'unique entier naturel d strictement inférieur à 40 tel que $3d \equiv 1\ [40]$.

3. La clé privée est $d = 27$. Calculer le reste de 14^d par la division euclidienne par 55.

4. Avec les mêmes paramètres p, q et c :
   a] Coder un nombre au choix.
   b] Décoder le nombre obtenu.

5. **a]** Montrer que, pour tout entier naturel a, on a $a^{81} \equiv a\ [5]$.
   b] En déduire que, pour tout entier naturel a, on a $a^{81} \equiv a\ [55]$.

Dans la pratique, le nombre N est bien plus grand que 55.
Le système RSA 1024 bits correspond à un nombre N de l'ordre de $2^{1024} \approx 10^{308}$.
C'est la difficulté à déterminer les deux nombres premiers dont le produit vaut N qui rend le système sûr.