HỘI TOÁN HỌC VIỆT NAM

THÔNG TIN TOÁN HỌC

Tháng 3 Năm 2003 Tập 7 Số 1

GS Ngô Thúc Lanh (ĐHSP Hà Nội)

Lưu hành nội bộ

Thông Tin Toán Học

• Tổng biên tập:

Đỗ Long Vân Lê Tuấn Hoa

• Hội đồng cố vấn:

Phạm Kỳ Anh Phan Quốc Khánh
Đinh Dũng Phạm Thế Long
Nguyễn Hữu Đức Nguyễn Khoa Sơn

• Ban biên tập:

Nguyễn Lê Hương Nguyễn Xuân Tấn
Lê Hải Khôi Lê Văn Thuyết
Tống Đình Quì Nguyễn Đông Yên

• Tạp chí **Thông Tin Toán Học** nhằm mục đích phản ánh các sinh hoạt chuyên môn trong cộng đồng toán học Việt nam và quốc tế. Tạp chí ra thường kì 4-6 số trong một năm.

• Thể lệ gửi bài: Bài viết bằng tiếng việt. Tất cả các bài, thông tin về sinh hoạt toán học ở các khoa (bộ môn) toán, về hướng nghiên cứu hoặc trao đổi về phương pháp nghiên cứu và giảng dạy đều được hoan nghênh. Tạp chí cũng nhận đăng các bài giới thiệu tiềm năng khoa học của các cơ sở cũng như các bài giới thiệu các nhà toán học. Bài viết xin gửi về toà soạn. Nếu bài được đánh máy tính, xin gửi kèm theo file (đánh theo ABC, chủ yếu theo phông chữ .VnTime).

• Quảng cáo: Tạp chí nhận đăng quảng cáo với số lượng hạn chế về các sản phẩm hoặc thông tin liên quan tới khoa học kỹ thuật và công nghệ.

• Mọi liên hệ với tạp chí xin gửi về:

Tạp chí: ***Thông Tin Toán Học***
Viện Toán Học
HT 631, BĐ Bờ Hồ, Hà Nội

e-mail:
lthoa@thevinh.ncst.ac.vn

BÀI TOÁN P = NP?
QUÀ TẶNG CỦA TIN HỌC GỬI TẶNG TOÁN HỌC

Phạm Trà Ân ***(Viện Toán học)***

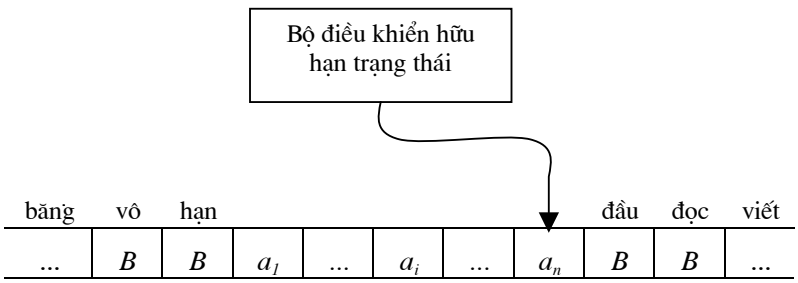
Nói một cách đại thể, bài toán **P = NP**? có thể phát biểu như sau : Có phải mọi ngôn ngữ chấp nhận được bởi một *thuật toán không-đơn định* với *thời gian đa thức* thì cũng chấp nhận được bởi một *thuật toán đơn định* nào đấy với *thời gian vẫn là đa thức*?

Về lịch sử, vấn đề **P = NP**? được đặt ra lần đầu tiên vào năm 1971 bởi S. Cook, một nhà toán học người Canada và hiện được coi là một trong những vấn đề chưa có lời giải nổi tiếng nhất trong Toán học. Bằng chứng là năm 1998, theo gương của D. Hilbert(1), nhà toán học Steve Smale(2), trong bài báo có nhan đề "Những vấn đề Toán học giành cho thế kỷ sau", đã xếp bài toán **P = NP**? ở vị trí thứ 3 trong số 18 bài toán quan trọng của thế kỷ XXI. Hơn thế nữa, ngày 24/5/2000, tại Paris, trước thềm của Thiên niên kỷ mới, Viện Toán học Clay, thuộc đại học Massachusetts, Cambridge (CMI) của Mỹ, đã công bố 7 bài toán được mệnh danh là "Các bài toán của thiên niên kỷ mới"(3) và treo giải thưởng 1.000.000 đô la cho lời giải của mỗi bài toán. Bài toán **P = NP**? chiếm vị trí thứ nhất trong danh sách 7 bài toán này.

Để phát biểu chính xác bài toán **P = NP**? ta cần đến một định nghĩa toán học cho khái niệm thuật toán và do đó cần đến một định nghĩa hình thức hóa của máy tính.

Mô hình chuẩn tắc của máy tính chính là mô hình máy Turing, do A. Turing(4), nhà toán học người Anh, đề xuất vào năm 1936, trước cả chục năm thời điểm chiếc máy tính điện tử đầu tiên xuất hiện. Ngày nay, máy Turing vẫn tiếp tục được coi là một mô hình toán học thích hợp nhất để diễn tả khái niệm thuật toán và khái niệm hàm tính được.

Máy Turing $\boldsymbol{M}$ gồm một bộ điều khiển với tập hữu hạn trạng thái Q và một đầu đọc-viết, chuyển động trên một băng vô hạn cả về 2 phía. Băng được chia thành từng ô, mỗi ô chứa một ký tự thuộc một bảng chữ hữu hạn Γ, bao gồm cả ký tự trắng b (blank). Mỗi máy $\boldsymbol{M}$ có một bảng chữ vào Σ, $\Sigma \subset \Gamma$ và $b \notin \Sigma$. Tại thời điểm bắt đầu hoạt động, dữ liệu vào của $\boldsymbol{M}$ là một dãy hữu hạn ký tự thuộc Σ, được ghi trên các ô liền nhau của băng, các ô còn lại của băng ghi ký tự trắng b, đầu đọc nhìn ký tự bên trái nhất của dãy ký tự vào và bộ điều khiển ở một trạng thái đặc biệt q_0, gọi là trạng thái ban đầu của $\boldsymbol{M}$, (xem hình dưới đây).



Tại mỗi bước hoạt động, máy $\boldsymbol{M}$ ở một trạng thái q, đầu đọc nhìn ô chứa ký tự s, máy sẽ có hoạt động phụ thuộc vào cặp (q,s) nhờ một hàm chuyển δ của máy. Hoạt động này bao gồm việc in một ký tự mới đè lên ký tự mà đầu đọc đang nhìn, chuyển đầu đọc sang trái hay sang phải một ô, đồng thời bộ điều khiển chuyển sang một trạng thái mới q'. Thí dụ $\delta(q, s) = (q', s', h)$ có nghĩa là $\boldsymbol{M}$ đang ở trạng thái q, nhìn ký tự s, $\boldsymbol{M}$ sẽ chuyển sang trạng thái q', ghi đè ký tự s' lên ký tự s, đầu đọc chuyển động sang phải một ô nếu $h = 1$, hoặc sang trái một ô nếu $h = -1$. Tập Q có chứa 3 trạng thái đặc biệt q_0, q_{cn}, q_{bb} (trạng thái *ban đầu*, trạng thái *chấp nhận*, trạng thái *bác bỏ*).

Một cách hình thức, *máy Turing* $\boldsymbol{M}$ là bộ bốn $\boldsymbol{M} = (\Sigma, \Gamma, Q, \delta)$.

Một hình trạng của $\boldsymbol{M}$ là một dãy xqy , với $x, y \in \Sigma^*$, $q \in Q$. Hình trạng $C = xqy$ diễn tả tình trạng $\boldsymbol{M}$ đang ở trạng thái q, trên băng có ghi dãy ký tự xy, đầu đọc đang nhìn ký tự bên trái nhất của y. Nếu C và C' là 2 hình trạng của $\boldsymbol{M}$, $C = xqsy$, $C' = xs'q'y$ và nếu $\delta(q,s) = (q', s', 1)$, thì ta nói $\boldsymbol{M}$ chuyển từ hình trạng C sang hình trạng C' và ký hiệu $C \overset{M}{\rightarrow} C'$. Tương tự cho trường hợp $h = -1$. Hình trạng $C = xqy$ là *dừng* nếu $q \in \{q_{cn}, q_{bb}\}$.

Một tính toán của $\boldsymbol{M}$ với dãy ký tự vào $\omega \in \Sigma^*$, là dãy hình trạng $C_0, C_1, \ldots, C_n, \ldots$ sao cho $C_0 = q_0\,\omega$, $C_i \overset{M}{\rightarrow} C_{i+1}$ và tận cùng bằng một hình tranh dừng nếu dãy là hữu hạn. Như vậy băng vô hạn có thể xem vừa như kênh vào-ra, vừa như một *bộ nhớ ngoài vô hạn tiềm năng* của máy $\boldsymbol{M}$.

Ta nói $\boldsymbol{M}$ *chấp nhận* dãy vào ω , nếu dãy tính toán của $\boldsymbol{M}$ với ω là dừng và hình trạng cuối cùng có chứa trạng thái chấp nhận q_{cn} . *Ngôn ngữ chấp nhận* bởi $\boldsymbol{M}$ là tập : $L(\boldsymbol{M}) = \{\omega \in \Sigma^* \mid \boldsymbol{M}$ chấp nhận $\omega\}$.

Ký hiệu $t_{\boldsymbol{M}}(\omega)$ là số các bước của tính toán $\boldsymbol{M}$ với dãy vào ω. Nếu tính toán này không dừng, ta đặt $t_{\boldsymbol{M}}(\omega) = \infty$. Với $n \in N$, ký hiệu $T_{\boldsymbol{M}}(n)$ là thời gian chạy máy của $\boldsymbol{M}$ trong trường hợp xấu nhất, tức là $T_M(n) = \max\{t_M(\omega) \mid \omega \in \Sigma^n\}$. Ta nói máy $\boldsymbol{M}$ *chạy trong thời gian đa thức*, nếu có tồn tại một đa thức $p(n)$, sao cho với mọi $n \in N$, $T_{\boldsymbol{M}}(n) \leq p(n)$. Bây giờ ta định nghĩa lớp $\mathbf{P}$ là tập :

$$\mathbf{P} = \{L \mid L = L(\boldsymbol{M}) \text{ với } \boldsymbol{M} \text{ là máy Turing thời gian đa thức}\}.$$

Máy Turing ta xét đến ở trên còn được gọi là *máy Turing đơn định* (vì hàm δ là đơn trị) để phân biệt với *máy Turing không-đơn định*, mà bây giờ chúng ta sẽ đề cập đến.

Đặc điểm của *máy Turing không-đơn định* là tại mỗi hình trạng bất kỳ, máy được phép có một số khả năng hành động (hàm chuyển δ là không đơn trị). Còn về các yếu tố khác, máy Turing không-đơn định được định nghĩa hoàn toàn như máy Turing đơn định . Ta định nghĩa lớp $\mathbf{NP}$ là tập :

$$\mathbf{NP} = \{L \mid L = L(M) \text{ với } \boldsymbol{M} \text{ là Turing không-đơn định thời gian đa thức}\}.$$

Chú ý rằng máy Turing không-đơn định vốn không được dự định để mô hình hoá các tính toán. Nó chỉ đơn thuần là một máy toán học bổ trợ và có thể hình dung như một máy dùng để kiểm chứng một phỏng đoán có là đúng hay không.

Đến đây ta có thể phát biểu chính xác bài toán **P= NP**? như sau : Tập **P** có bằng tập **NP** hay không? Hiển nhiên là **P** $\subseteq$ **NP**, nhưng chúng ta không biết bao hàm thức trên có là thật sự hay không?

Một cách hoàn toàn tương đương, ta có thể hiểu **P** là lớp các bài toán có thể giải được trong thời gian đa thức, còn **NP** là lớp các bài toán, mà mọi nghiệm giả định đều có thể được kiểm chứng trong thời gian đa thức. Thường thì việc tìm nghiệm khó hơn nhiều so với việc kiểm chứng nghiệm. Thí dụ ta xét bài toán người bán hàng rong ở dạng sau: dữ liệu vào gồm khoảng cách giữa mọi cặp thành phố và thêm một số *T*, được gọi là "số mục tiêu". Nếu bài toán là hãy tìm một hành trình của người bán hàng rong có độ dài nhỏ hơn hay bằng *T* thì đó là một bài toán rất khó. Nhưng nếu ở dạng cho trước một hành trình của người bán hàng rong, hỏi độ dài của hành trình đã cho đó có nhỏ hơn hay bằng số *T* hay không thì bài toán lại ở dạng dễ hơn rất nhiều.

Về nguồn gốc, bài toán có xuất xứ từ Tin học. Đó là vào những năm 60 của thế kỷ XX. Các máy tính bắt đầu được sử dụng rộng rãi để giải các bài toán khoa học-kỹ thuật, và các bài toán kinh tế. Các nhà tin học đứng trước một vấn đề chưa có câu trả lời: Thế nào là một thuật toán "tốt", một thuật toán "không tốt"? Thế nào là một bài toán "dễ", một bài toán "khó"? Vào thời điểm này, các nhà tin học mới chỉ có khái niệm "trực quan" và phần nào "cực đoan" khi coi một thuật toán là "tốt" nếu thời gian chạy máy trong thực tế phải là khá nhanh (nhưng lại không đòi hỏi nó phải chạy khá nhanh đối với mọi dữ liệu đầu vào có thể có). Mãi cho đến năm 1965, J. Edmonds lần đầu tiên đưa ra ý tưởng mới: một thuật toán được coi là tốt, nếu thời gian chạy máy bị chặn bởi một đa thức theo kích thước của mọi dữ liệu vào (kể cả trường hợp xấu nhất). Một bài toán được coi là dễ nếu có thuật toán thời gian đa thức giải nó. Như vậy Edmonds đã cho một ranh giới rõ ràng giữa tính "dễ" và "khó" của một bài toán, giữa tính "tốt" và "không tốt" của một thuật toán: trong **P** là dễ và tốt, ngoài **P** là khó và không tốt. Thực ra, đối với một thuật toán có thời gian chạy máy bị chặn bởi một đa thức bậc "khổng lồ", chẳng hạn bởi n^{100}, thì độ khó của nó cũng chẳng kém gì hàm mũ. Tuy nhiên, việc phân chia ranh giới giữa tính dễ và tính khó, giữa tính tốt và tính không tốt bên trong lớp **P** là không tự nhiên. Một định nghĩa như vậy sẽ luôn luôn bị thay đổi theo thời gian cùng với sự phát triển nhanh chóng đến kỳ diệu của các thế hệ máy tính (người ta đã thống kê cứ sau 18 tháng tốc độ máy tính được tăng gấp đôi và cứ sau 10 năm thì số lượng máy tính cũng tăng gấp đôi). Nhưng khi bắt tay vào xem xét cụ thể nhiều bài toán tối ưu tổ hợp, cho dù các nhà nghiên cứu đã rất kiên trì, nhưng họ vẫn không tìm được các *thuật toán đơn định* chạy trong thời gian đa thức, trong khi đó nếu cho phép dùng *thuật toán không đơn định* thì lại dễ ràng chỉ ra các thuật toán chạy trong thời gian đa thức. Vì vậy lúc đầu các nhà tin học giả định **P** $\neq$ **NP**. Nhưng chứng minh mãi không được, thì một cách tự nhiên, giả định ngược lại **P = NP** được đặt ra và sau đó bài toán được chuyển đến các nhà toán học để chính xác hoá toán học. Bằng công cụ máy Turing, các nhà toán học đã phát biểu lại chính xác toán học bài toán như đã trình bầy ở phần trên và nó trở thành một bài toán độc lập và quen thuộc của Lý thuyết Ngôn ngữ hình thức. Qua 30 năm tồn tại, bài toán **P = NP?** ngày càng tỏ ra là một "viên ngọc quý" theo các tiêu chí sau: Một là phát biểu bài toán rất đơn giản, nhưng lại hoàn toàn chính xác về mặt Toán học. Hai là qua thời gian, cộng đồng các nhà toán học đều thừa nhận đây là một bài toán khó, thậm chí rất khó. Ba là các nhà toán học có uy tín trên thế giới đều cho rằng việc giải quyết bài toán , và ngay cả các nghiên cứu có liên quan đến bài toán, cho dù không đi đến kết quả cuối cùng, cũng sẽ góp phần thúc

đẩy sự phát triển của Toán học trong thế kỷ XXI. Chính vì vậy, bài toán đã lọt vào "mắt xanh" của các nhà toán học của Viện Toán Clay và của nhà toán học nổi tiếng Steve Smale. Giờ đây, khi mà bài toán **P = NP**? đã trở thành một trong số các bài toán nổi tiếng nhất và đắt giá nhất trong lịch sử Toán học (còn đắt giá hơn một giải thưởng Nobel!), song các nhà toán học vẫn nhớ đến nguồn gốc của bài toán và vẫn coi bài toán như là một quà tặng quý giá, thể hiện mối quan hệ cộng tác qua lại giữa Toán học và Tin học, mà Tin học đã tin tưởng gửi tặng Toán học.

Trở lại với các khía cạnh toán học của bài toán , để nghiên cứu sâu hơn mối quan hệ giữa **P** và **NP**, có cả một lý thuyết gọi là "*Lý thuyết về tính NP-đầy đủ*", mà sau đây ta sẽ phác họa một vài nét cơ bản. Ý tưởng của phương pháp này rất đơn giản. Vì đã có $\mathbf{P} \subseteq \mathbf{NP}$ rồi, nên việc xét quan hệ giữa **P** và **NP** nói chung là phải duyệt toàn bộ lớp **NP**. Thay cho việc duyệt toàn bộ lớp **NP**, ta chỉ muốn duyệt một bộ phận nhỏ, thậm chí chỉ một bài toán trong **NP** mà thôi. Muốn thế ta hãy chọn ra bất kỳ một bài toán "*khó giải nhất*" C trong lớp **NP** theo một nghĩa nào đấy rồi kiểm tra xem C có thuộc **P** hay không. Nếu $C \in \mathbf{P}$, thì vì C đã là bài toán khó nhất rồi, ta suy ra các bài toán còn lại, vì ít khó hơn hay cùng lắm cũng chỉ khó bằng C, cũng sẽ phải thuộc **P**, do đó ta có **P = NP**. Còn nếu như C không thuộc lớp **P** thì đó đã là bằng chứng của $\mathbf{P} \subset \mathbf{NP}$. Như vậy mỗi bài toán "khó nhất" trong **NP** lại là một "chìa khóa" để giải bài toán **P = NP**? S. Cook gọi các "bài toán khó nhất trong **NP**" này là các "*bài toán NP-đầy đủ*". Vấn đề còn lại là định nghĩa như thế nào là bài toán A là "*khó hơn*" bài toán B và thế nào là bài toán C là khó nhất trong lớp **NP**? Để giải quyết vấn đề này, ta có thể vận dụng khái niệm *Turing-dẫn* trong lý thuyết thuật toán.

Định nghĩa 1. *Giả sử L_i là ngôn ngữ trên bảng chữ Σ_i , $i = 1, 2$. Khi đó $L_1 \leq_p L_2$ (L_1 là p-dẫn được về L_2) nếu và chỉ nếu có một hàm tính được trong thời gian đa thức $f: \Sigma_1^* \to \Sigma_2^*$ sao cho :*

$$x \in L_1 \Leftrightarrow f(x) \in L_2 \text{ , với mọi } x \in \Sigma_1 .$$

Về ý nghĩa, nếu $L_1 \leq_p L_2$ thì L_2 là khó hơn L_1, vì giải được bài toán L_2 sẽ giải được bài toán L_1, ngược lại nói chung là không có.

Định nghĩa 2. *Ngôn ngữ L là NP-đầy đủ nếu và chỉ nếu $L \in \mathbf{NP}$ và với mọi $L' \in \mathbf{NP}$ thì $L' \leq_p L$.*

Về ý nghĩa, nếu L là NP-đầy đủ thì L là khó nhất trong lớp **NP** , vì giải được L sẽ giải được mọi bài toán L' khác trong **NP**, nhưng ngược lại không đúng.

Ta có các mệnh đề sau đây :

Mệnh đề 1. *Nếu $L_1 \leq_p L_2$ và $L_2 \in \mathbf{P}$, thì $L_1 \in \mathbf{P}$.*

Chứng minh dùng định nghĩa của phép dẫn $\leq_p$.

Mệnh đề 2. *Nếu L_1 là NP-đầy đủ, $L_2 \in \mathbf{NP}$ và $L_1 \leq_p L_2$, thì L_2 là NP-đầy đủ.*

Chứng minh dùng tính bắc cầu của quan hệ $\leq_p$.

Về ý nghĩa, Mệnh đề 2 cho một phương pháp cơ bản để chứng minh một bài toán mới là NP-đầy đủ.

Mệnh đề 3. *Nếu L là NP-đầy đủ và* $L \in P$ *thì* $P = NP$.

Chứng minh dùng Mệnh đề 1.

Về ý nghĩa, Mệnh đề 3 là một con đường nhằm hướng đích **P = NP**.

Tuy nhiên để áp dụng Mệnh đề 2, ta còn cần có cái bắt đầu, tức là cần một ngôn ngữ đầu tiên là NP-đầy đủ. Vinh dự đó thuộc về một bài toán quyết định trong Lôgic boole , do Cook chứng minh vào năm 1971 và thường được gọi là bài toán SATISFIABILITY hay ngắn gọn là bài toán SAT với nội dung như sau: F là một công thức mệnh đề cho trước. Hỏi F có là thỏa được hay không?

Mệnh đề 4 (Định lý Cook*). SATISFIABILITY là NP-đầy đủ.*

Một năm sau đó, dựa vào phương pháp của Cook, M. Karp đã chỉ ra một loạt 20 bài toán tối ưu tổ hợp dạng cổ điển là NP-đầy đủ, tiếp theo L. Levin đã chỉ ra 6 bài toán nữa là NP-đầy đủ. Sau đó là thời kỳ hoàng kim của NP-đầy đủ, số lượng các bài toán NP-đầy đủ được phát hiện tăng nhanh. Đến năm 1979, hai tác giả M. Garey và D. Johnson[5] , trong một quyển sách được coi là sách gối đầu giường của "các nhà **P = NP?**" , đã tổng kết được 300 bài toán là NP-đầy đủ. Từ đó đến nay, con số này vẫn tăng hàng năm. Sự phong phú và đa dạng của các bài toán NP-đầy đủ là một thuận lợi trong việc chọn "chìa khóa" để mở "cánh cửa" **P = NP?**

Cách đây 30 năm, con đường dẫn đến bài toán **P = NP?** đã rộng mở và mới hấp dẫn làm sao! Nhiều nhà toán học, nhiều nhà tin học lý thuyết đã xắn tay áo vào cuộc . Người ta tìm trong danh sách các bài toán NP-đầy đủ, mỗi người tự chọn lấy cho mình một bài toán mình am hiểu nhất, hoặc là gần với chuyên môn của mình nhất, thậm chí chỉ đơn thuần là mình thấy thích nhất. Người ta lục trong "kho vũ khí toán học" lấy ra các thuật toán thời gian đa thức (có một đống các thuật toán như vậy, chẳng hạn như thuật toán "háu ăn" , các thuật toán qui hoạch động, các thuật toán dẫn về bài toán quy hoạch tuyến tính, v . . .v . . .). Người ta ướm thử, sử dụng thử, gá lắp thêm, cải tiến thêm, rồi sáng tạo , nhằm có được một thuật toán giải được bài toán mình đã chọn chỉ trong thời gian đa thức. Nếu có được một thuật toán như vậy, sẽ suy ra **P = NP**. Nhưng tiếc thay, tất cả các nỗ lực đều không đi đến kết quả. Chứng minh mãi **P = NP** không được, người ta quay ra chứng minh **P ≠ NP**. Nhưng các cố gắng bỏ ra cũng chẳng may mắn gì hơn. Đây đó đã có người nghi ngờ: Phải chăng các kỹ thuật chứng minh mà ta hiện có, không đủ để chứng minh **P = NP** mà cũng chẳng đủ để chứng minh **P ≠ NP**?

Bất chấp sự nỗ lực phi thường của bầy chú lùn - Các nhà toán học, nàng Bạch tuyết "**P = NP?**□ vẫn chìm trong giấc ngủ. Hình như Nàng còn đang đợi một chàng Hoàng tử - một ý tưởng toán học hoàn toàn mới mẻ - từ phương trời xa tới để đánh thức Nàng dậy?

Trong khi chờ đợi chàng Hoàng tử đến cứu nàng Bạch tuyết, ta hãy thử hỏi điều gì sẽ xảy ra nếu như **P = NP**, và nếu như **P ≠ NP**?

Nếu như **P ≠ NP**, các điều sau đây sẽ xẩy ra:

- *Độ mật của các hệ mã khóa công khai* dựa trên giả thiết **P ≠ NP** sẽ được khẳng định. Do vậy mã khóa công khai sẽ được triển khai rộng rãi hơn, phù hợp với xu thế phát triển thương mại điện tử của xã hội trong tương lai.

• Các bài toán NP-đầy đủ trở thành các *bài toán bất trị* vô phương "cứu chữa", cho đến khi có một cuộc cách mạng mới trong Tin học cùng với việc xuất hiện một thế hệ máy tính hoàn toàn mới về nguyên lý hoạt động, có khả năng "siêu" tăng tốc. Cuộc cách mạng ấy nhất định sẽ đến, nhưng bao giờ nó đến thì chưa rõ, chỉ biết rằng giờ đây, ở phía chân trời xa, đã bắt đầu thấy những tia chớp đầu tiên. Đó là những ý tưởng táo bạo của các nhà toán học và các nhà vật lý lý thuyết về một thế hệ máy tính mới, có tên là *máy tính lượng tử*. Các máy tính lượng tử sẽ hoạt động theo các nguyên lý chung của Cơ học lượng tử. Năm 1997, P. Shor đã công bố một thuật toán chạy trên máy tính lượng tử giải bài toán phân tích một số nguyên thành các thừa số nguyên tố trong thời gian đa thức, điều mà máy Turing chỉ có thể làm được với thời gian mũ. Tuy nhiên các máy tính lượng tử hiện nay mới chỉ có trên giấy. Chắc là phải còn xa nữa mới tới thời điểm chiếc máy tính lượng tử đầu tiên được đặt lên bàn làm việc của các nhà nghiên cứu.

Còn nếu như **P = NP**, ta sẽ có các hệ quả trực tiếp sau đây:

• Mọi bài toán hễ kiểm chứng dễ thì giải cũng dễ.

• Tất cả các bài toán tối ưu tổ hợp thông thường đều giải được trong thời gian đa thức.

• Mối lo "Bùng nổ tổ hợp" bấy lâu nay vẫn canh cánh trong lòng, nay bỗng không còn nữa.

• Một loạt các hệ mã khoá công khai dựa trên giả thiết **P ≠ NP** bị đổ vỡ, trong số này có các hệ mã quan trọng, mang tính toàn cầu, thí dụ như hệ mã hoá truyền dữ liệu DES (Data Encryption Standard), hệ thanh toán tài chính trên INTERNET.

Ta có cảm giác sững sờ, nuối tiếc, vì thế giới quanh ta bỗng chốc nghèo đi, đơn điệu đi! Ta chợt hiểu và đồng cảm với M. Garey và D. Johnson[5], khi các ông viết: "Thiện chí của hầu hết các nhà nghiên cứu là mong muốn **P ≠ NP**". Còn S. Cook, cha đẻ của bài toán **P = NP**?, thì lý trí hơn khi khẳng định: "Hầu hết các nhà toán học đều tin rằng **P ≠ NP**". Từ nước Phần lan lạnh, A. Salomaa - nguyên chủ tịch Hội Tin học lý thuyết Châu Âu - đã gửi đến nước Việt nam nóng bức thông điệp: Xin hãy bình tâm, "ngày càng có nhiều người tin rằng **P ≠ NP**" .

Ta cảm nhận được hơi ấm của bàn tay bè bạn khắp bốn phương!

Chú thích

(1) D. Hilbert (1862-1943), là nhà toán học nổi tiếng người Đức. Năm 1900, Ông được mời đọc một báo cáo toàn thể tại Đại hội Toán học thế giới. Thay cho việc đọc báo cáo, Ông đưa ra một danh sách 23 bài toán khó chưa có lời giải, coi như là những thách thức của thế kỷ XIX chuyển giao cho thế kỷ XX. Các bài toán này, sau được gọi với cái tên chung là các bài toán Hilbert và được đánh số từ 1-23. Cho đến nay, hầu hết các bài toán Hilbert đã được giải quyết và quá trình giải chúng đã thực sự thúc đẩy sự phát triển Toán học ở thế kỷ XX.

(2) Steve Smale, sinh năm 1930, tiến sĩ toán tại đại học Michigan năm 1957, giáo sư đại học California Berkeley, giải thưởng Fields. "Những vấn đề Toán học giành cho thế kỷ sau" đăng ở tạp chí: The mathematical Intelligencer, tập 20 (1998), gồm: 1) Giả thuyết Rieman; 2) Giả thuyết Poincaré; 3) Bài toán **P=NP?**; 4) Các không điểm nguyên của một đa thức; 5) Các giới hạn chiều cao của đường cong Diophant; 6) Tính hữu hạn của số các cân bằng tương đối trong cơ học vũ trụ; 7) Phân bố các điểm trên 2-hình cầu; 8) Đưa động lực học vào lý thuyết kinh tế; 9) Vấn đề quy hoạch tuyến tính; 10) Bổ đề đóng kín; 11) Động lực học một chiều là hyperbol tổng quát; 12) Nhóm con trung tâm của các vi đồng phôi; 13) Bài toán Hilbert thứ 16; 14) Điểm hấp dẫn Lorenz;

15) Các phương trình Navier — Stokes; 16) Giả thuyết Jacobi; 17) Giải các phương trình đa thức; 18) Giới hạn của trí tuệ (xem chi tiết trong Thông tin Toán học, số sắp tới).

(3) Bẩy bài toán của thiên niên kỷ mới là: 1) Bài toán **P = NP?**; 2) Giả thuyết Hodge; 3) Giả thuyết Poincaré; 4) Giả thuyết Riemann; 5) Sự tồn tại các nghiệm với ý nghĩa "lỗ hổng khối lượng" của phương trình Yang-Mills; 6) Sự tồn tại nghiệm trơn của phương trình Navier-Stokes; 7) Giả thuyết Birch và Swinnerton-Dyer (xem chi tiết trong Thông tin Toán học, Tập 5 Số 1(2001)).

(4) A. Turing (1912 - 1966), là nhà toán học người Anh. Năm 1936, Ông đã xây dựng mô hình máy tính, sau này được gọi là máy Turing, nhằm chính xác hoá khái niệm thuật toán. Trong Chiến tranh thế giới 2, Ông tham gia nhóm các nhà khoa học chuyên thám các mật mã của phát xít Đức. Ông đã thành công trong việc chế tạo ra một máy giải mã tự động, giải một lớp mã quan trọng của quân đội Đức. Tất cả các điều này, người ta chỉ được biết sau khi Ông đã mất. Năm 1999, Ông được tạp chí Times bình chọn là một trong số 20 nhà khoa học có ảnh hưởng nhất của thế kỷ XX.

(5) M. Garey and D. Johnson. *Computers and Intractibility, a Guide to the Theory of NP-Completeness.* W. H. Freeman and Co., San Francisco, 1979.

Sách nổi tiếng vì có phần tổng kết 300 bài toán là NP-đầy đủ.

Hệ mã RSA có thể bị công phá bằng "chip" chuyên dụng!

Phạm Huy Điển (*Viện Toán học*)

Mọi người đều biết "cái mạnh" của hệ mã hóa công khai RSA là dựa trên "điểm yếu" của máy tính trong việc phân tích một số nguyên (đủ lớn) ra các thừa số nguyên tố. Cách đây chưa đầy 10 năm (chính xác là năm 1994), để phân tích được một hợp số gồm 129 chữ số thập phân ra các thừa số nguyên tố (nhằm giải mã một câu được mã hoá bởi hệ RSA), người ta phải dùng tới 1600 máy tính mạnh (bao gồm đủ các loại *workstations, mainframes, và supercomputers*) làm làm việc liên tục trong vòng 8 tháng. Hiện nay, phương pháp được xem là hiệu quả nhất đối với bài toán này là thuật toán sử dụng "sàng trường số". Chính bằng phương pháp này mà gần đây (năm 1999) người ta đã phân tích được hợp số với độ dài kỷ lục là 155 chữ số thập phân (512 bit nhị phân), nhưng cũng mất nhiều tháng ròng và với số lượng máy tính khổng lồ. Cho nên hệ mã RSA chuẩn mực, với độ dài chìa khoá 1024 bít nhị phân (khoảng 308 chữ số thập phân), được xem là "bất khả bẻ" trong vòng 15-20 năm nữa. Trong suốt hơn 20 năm tồn tại đã qua (kể từ khi được công bố váo năm 1977), hệ mã RSA đã bị rất nhiều người tìm đủ mọi cách "tấn công", nhưng nó vẫn đứng vững. Kết quả hơn 20 năm "công phá" của giới "thám mã chuyên nghiệp" đã được tóm lược trong bài báo của Dan Boneh với tựa đề "Hai mươi năm tấn công hệ mã RSA" (đăng trong tờ *Notices of the AMS*, tháng 2, năm 1999), trong đó thừa nhận rằng RSA chỉ có thể bị "bẻ" khi người ta không biết dùng nó một cách "bài bản" mà thôi. Ta hiểu vì sao RSA trở thành hệ mã thông dụng nhất trong các hệ mã "phi đối xứng" cho đến tận bây giờ.

Thế mà mới đây Adi Shamir (một trong 3 đồng tác giả đã công bố phát minh hệ mã RSA) làm cho "thiên hạ" giật mình khi tuyên bố rằng ông đã cùng các cộng sự tại phòng Tin học và Toán ứng dụng của Viện nghiên cứu khoa học Weizmann (Israel) thiết kế ra "con chip đặc chủng" cho việc phân tích một số ra các thừa số nguyên tố, có sức mạnh phi thường và có khả năng bẻ được hệ mã RSA tiêu chuẩn hiện nay. Một công cụ "đặc chủng" kiểu này cũng đã từng được biết đến trước đây, đó là hệ thống quang điện tử TWINKLE, sử dụng các thành phần khá đắt tiền và khó chế tạo. Hệ thống mới của Shamir và các đồng nghiệp, gọi tắt là TWIRL, có nhiều điểm giống với TWINKLE, nhưng không chứa các thành phần quang học đắt tiền, khó kiếm mà được thiết lập dựa trên công nghệ VLSI phổ biến hiện nay, với cấu trúc song song hữu hiệu hơn (cho chính bài toán phân tích số). Về bản chất nó là một hệ thống tích hợp một lượng khổng lồ các bộ vi xử lý chạy trên tần số 1GHz.

Cho tới lúc này, "con chip đặc chủng" TWIRL mới chỉ nằm trên sơ đồ, chưa được triển khai trong thực tế, nhưng một số đánh giá sơ bộ cho thấy: để phân tích một số có "độ dài kỷ lục" 512 bit nhị phân (như đã nói ở trên) chỉ cần một máy tính chuyên dụng thiết lập trên cơ sở con chip TWIRL trị giá khoảng 10 ngàn USD, làm việc trong vòng 10 phút. Nếu nhớ rằng công việc này đã từng đòi hỏi hàng ngàn máy tính mạnh làm việc trong nhiều tháng ròng rã, ta thấy ngay sức mạnh của "con chip chuyên dụng" quả là phi thường. Tuy nhiên, cũng theo các đánh giá này, muốn phân tích một số có độ dài gấp đôi như thế, tức là khoảng 1024 bit nhị phân (như chìa khoá thông thường của một hệ mã RSA tiêu chuẩn hiện nay), thì phải cần tới một máy chuyên dụng trị giá khoảng 10 triệu USD, làm việc liên tục trong thời gian 1 năm. Như vậy, giả sử cứ theo cái đà này mà tiếp tục được, thì để bẻ được hệ mã RSA với độ dài khoá 2048 bit nhị phân thì phải cần tới máy tính chuyên dụng trị giá 10 tỷ USD, làm việc liên tục trong 52560 năm! (Tuy nhiên điều "giả sử" này cũng khó mà thành hiện thực, vì trong thiết kế của chip thì con số 1024 có vẻ như là một cái "ngưỡng" về mặt phần cứng mà chưa thấy khả năng nào có thể "nâng" được lên cao hơn một cách đáng kể. Dù rằng các tác giả có đề cập tới việc thiết kế các chip đặc thù cho việc phân tích các hợp số đủ mịn, chứa các thừa số nguyên tố không vượt quá 10 chữ số thập phân, và hy vọng nó cho phép phân tích được các hợp số có độ dài tới 4096 bit, nhưng công nghệ này không áp dụng được cho trường hợp chung.)

Hiện nay, mặc dù chưa ai trông thấy cái máy chuyên dụng trị giá 10 triệu USD của Shamir và đồng nghiệp ra làm sao, những người "lo xa" đã bắt đầu chuyển sang dùng chìa khóa với độ dài lớn hơn (chịu thiệt phần nào về tốc độ xử lý), còn những người "thực tế" hơn thì vẫn yên tâm chờ cho cái máy chuyên dụng kia xuất hiện, để rồi dùng giải pháp thay đổi chìa hàng năm mà không muốn chịu hy sinh về mặt tốc độ.

Vừa qua, các cán bộ của phòng Nghiên cứu và Phát triển Phần mềm (Viện Toán học) đã tiến hành cho chạy thử phiên bản RSA mới với độ dài chìa khóa lên tới 2048 bit thì thấy rằng, trong các dịch vụ cơ bản của RSA hiện nay là *mã chìa khóa phiên* và *tạo chữ ký điện tử,* sự chênh lệnh về tốc độ xử lý so với phiên bản tiêu chuẩn (độ dài chìa khoá 1024 bit) là không đáng kể (nếu dùng các máy có cấu hình thông thường hiện nay, như Pentium III hoặc tương đương).

Xem ra, con "chip" của Shamir dù có là cái "móng tay rất nhọn" nhưng vẫn khó mà đâm thủng được vỏ "quả bưởi" RSA.

Chúc mừng Nhà giáo nhân dân, Giáo sư Ngô Thúc Lanh 80 tuổi

Bùi Văn Nghị *(ĐHSP Hà Nội)*

Giáo sư Ngô Thúc Lanh tham gia công tác trong ngành giáo dục từ năm 1947. Năm 1954, GS. Ngô Thúc Lanh là cán bộ giảng dạy của Ban Toán - Lý (tiền thân của khoa Toán - Tin, trường ĐHSP Hà Nội ngày nay) tại trường Sư phạm cao cấp ở Khu học xá Nam Ninh (Quảng Tây, Trung Quốc). GS. Ngô Thúc Lanh là một trong những cán bộ giảng dạy có mặt ngay từ những ngày đầu thành lập khoa Toán- Lý, trường Đại học sư phạm.

Trải qua các cương vị công tác: Cán bộ giảng dạy (từ năm 1954 đến năm 1958), Chủ nhiệm bộ môn Đại số (từ năm 1958 đến năm 1966), Chủ nhiệm khoa Toán (từ năm 1966 đến năm 1972), GS. Ngô Thúc Lanh luôn là người thầy giáo mẫu mực, người lãnh đạo tận tụy với công việc, có nhiều đóng góp lớn lao cho quá trình xây dựng và phát triển khoa Toán trường ĐHSP Hà Nội trong những năm 50, 60, 70, 80.

Nhiều sự kiện quan trọng gắn liền với những năm tháng giảng dạy và lãnh đạo khoa Toán, trường ĐHSP Hà Nội của GS. Ngô Thúc Lanh. Đó là những năm tháng còn rất thiếu đội ngũ cán bộ giảng dạy của những ngày đầu mới thành lập Khoa và Trường, những năm tháng chiến tranh phá hoại bằng không quân của giặc Mỹ, khoa Toán, trường ĐHSP Hà Nội phải đi sơ tán về Phù Cừ (Hưng Yên), Ứng Hoà (Hà Tây), về Vĩnh Tường (Vĩnh Phú). Đó là những năm tháng đầy khó khăn, vất vả trong cả việc chung lẫn việc tư của GS. Ngô Thúc Lanh. Năm học 1966-1967, năm đầu tiên của nhiệm kỳ Chủ nhiệm khoa Toán của GS Ngô Thúc Lanh, tổ Phổ thông chuyên toán (tiền thân của Khối Phổ thông chuyên Toán- Tin, trường ĐHSP Hà Nội ngày nay) được thành lập và cũng từ năm đó Khối đã liên tục dành được nhiều thành tích xuất sắc trong việc đào tạo, bồi dưỡng những học sinh năng khiếu về Toán. Cũng bắt đầu từ năm học này Khoa Toán có chủ trương mở chế độ bồi dưỡng cấp hai cho cán bộ giảng dạy (nay gọi là chế độ nghiên cứu sinh). Đặc biệt, trong nhiệm kỳ Chủ nhiệm khoa của GS Ngô Thúc Lanh, năm 1968, Khoa Toán vinh dự được Nhà nước công nhận là Khoa Lao động Xã Hội Chủ Nghĩa.

Trong những năm công tác tại Khoa Toán, trường ĐHSP Hà Nội, GS Ngô Thúc Lanh đã viết nhiều giáo trình, sách chuyên khảo, sách giáo khoa phục vụ cho giảng dạy ở nhiều trường trong cả nước. Rất nhiều các thế hệ học trò của GS Ngô Thúc Lanh đã trưởng thành, trở thành các nhà lãnh đạo cao cấp, các nhà khoa học có trình độ cao, các giáo sư, phó giáo sư, tiến sĩ khoa học, tiến sĩ..., các thầy giáo, cô

giáo giảng dạy ở các trường đại học, cao đẳng, các trường phổ thông. Hiện nay GS Ngô Thúc Lanh vẫn có những đóng góp quý báu, chỉ giáo cho các thế hệ kế tiếp. Giáo sư đã dành hết tâm huyết cho sự nghiệp giáo dục và đào tạo. Giáo sư rất xứng đáng với những danh hiệu: Nhà giáo nhân dân do Nhà nước trao tặng.

Nhân dịp Nhà giáo nhân dân, Giáo sư Ngô Thúc Lanh, 80 tuổi, xin kính chúc Giáo sư luôn luôn mạnh khoẻ và hạnh phúc.

CHÚC MỪNG GIÁO SƯ NGÔ THÚC LANH TRÒN 80 TUỔI

Vũ Tuấn ***(ĐHSP Hà Nội)***

Sau Cách mạng tháng Tám, như bao thanh niên khác, anh Ngô Thúc Lanh, sinh viên trường Đại học Đông Dương "xếp bút nghiên" lên đường tham gia cuộc kháng chiến chống Pháp bảo vệ Tổ quốc.

Anh không ra mặt trận. Theo đề nghị của giáo sư Ngụy Như Kontum, Bộ Giáo dục phân công anh dạy học. Nghiệp làm thầy đến với anh tình cờ như thế.

Đầu tiên, anh dạy ở trường Trung học kháng chiến Chu Văn An ở Việt Bắc, bậc học cao nhất ở chiến khu lúc ấy. Thời bấy giờ, trường ở trong lòng dân, thầy, trò ở nhà dân, rồi mới tự mình xây dựng trường sở và nơi ăn chốn ở riêng. Nhiều môn học, nhất là những môn học tự nhiên, các bài giảng chỉ nhờ vào trí nhớ của thầy và một vài quyển sách tiếng Pháp ngẫu nhiên có được, nhưng nhà trường đã hoạt động hết sức hăng hái, nghiêm túc và hiệu quả. Kết thúc khóa học mỗi người nhận một nhiệm vụ mới: vào công binh xưởng, ra mặt trận, vào địch hậu...Anh Lanh được điều động sang dạy học tại Khu học xá Trung ương ở Nam Ninh- Trung Quốc.

Hòa bình lập lại (1954) các trường đại học non trẻ của ta ra đời, anh lại là một trong những người xây nền móng cho cả hệ thống đại học Việt Nam sau này. Cùng với các giáo sư Lê Văn Thiêm, Nguyễn Thúc Hào, Hoàng Tụy, Nguyễn Cảnh Toàn... giáo sư Ngô Thúc Lanh đã tham gia xây dựng chương trình, viết giáo trình và giảng dạy rất nhiều môn toán khác nhau. Những người thầy đại học đầu tiên ấy đã đào tạo nhiều lớp cán bộ giảng dạy và nghiên cứu Toán học làm nòng cốt cho các trường đại học và các viện nghiên cứu ngày nay.

Từ năm 1956, hai giáo sư Ngô Thúc Lanh và Nguyễn Cảnh Toàn được giao nhiệm vụ xây dựng khoa Toán, trường Đại học Sư phạm Hà Nội. Từ đó GS Ngô Thúc Lanh đã cần mẫn làm việc, giảng dạy, đào tạo lớp lớp cán bộ Toán cho trường ĐHSP Hà Nội. Không được cử đi đào tạo chính quy ở nước ngoài như nhiều người khác, thầy phải tự học, tự đào tạo để hoàn thành mọi nhiệm vụ, lúc nào cũng rất cao, rất nặng nề.

Những năm thầy làm chủ nhiệm khoa là những năm khoa Toán ĐHSP Hà Nội làm việc nghiêm túc nhất, dạy dỗ chuẩn mực, học tập và lao động hăng say nhất, mặc dù đó là những năm gian khổ của thời bom đạn chống Mỹ.

Thầy đã dạy nhiều nghìn giờ, viết nhiều nghìn trang sách và đã có nhiều nghìn học trò.

Tận tụy, khiêm nhường và trung thực là bài học lớn thầy để lại trong lòng học trò.

Thời gian trôi đi...

Ngày nào còn là anh thanh niên sung sức, nhiệt huyết, hôm nay giáo sư Ngô Thúc Lanh đã bước sang tuổi 80. Còn mạnh mẽ, minh mẫn; vẫn hăng hái luyện

tập, đọc và viết. Đó là phúc ấm của riêng thầy.

Mỗi người có một cuộc đời. Có những người danh vọng chói chang. Rất nhiều cuộc đời khác trôi qua bình lặng, không ồn ào. Bình dị, liêm khiết và cần cù là cuộc đời nhà giáo. Thanh thản, hồn hậu là tâm hồn nhà giáo.

Kính chúc thầy cô mạnh khỏe, sống lâu vui hưởng tuổi già êm ả trời cho.

Quỹ Lê Văn Thiêm

Để góp phần khuyến khích các tài năng trẻ học toán và lựa chọn toán học làm nghề nghiệp tương lai của mình, Hội Toán học Việt nam đã thành lập ***Quỹ Lê Văn Thiêm*** và ***Giải thưởng Lê Văn Thiêm*** giành cho học sinh và giáo viên dạy toán ở các trường PTTH. Từ khi thành lập, Quỹ đã nhận được sự ủng hộ nhiệt tình của nhiều cơ quan, tổ chức và cá nhân các nhà khoa học trong và ngoài nước, và đã góp phần nhất định vào việc khuyến khích phong trào dạy toán, học toán ở các trường phổ thông.

Để có thể duy trì và phát triển Quỹ Lê Văn Thiêm, Hội Toán học Việt Nam rất mong nhận được sự ủng hộ tiếp tục của các cơ quan, đoàn thể và cá nhân

Xin chân thành cám ơn.

Quỹ Lê Văn Thiêm

Danh sách các tập thể và cá nhân đã ủng hộ quỹ Lê Văn Thiêm

(xếp theo thứ tự thời gian)

1. Đoàn Quang Mạnh, Trường Năng khiếu Hải Phòng
2. Nguyễn Vũ Quốc Hưng, ĐHQG HN
3. Đặng Đình Áng, ĐHQG TP HCM
4. Nguyễn Đình Trí, ĐHBK HN
5. Nguyễn Đình Lân, ĐHSP TP HCM
6. Trần Mạnh Hưng, CĐSP TP HCM
7. Nguyễn Thanh Vân, ĐH Toulouse, Pháp
8. Nguyễn Đình Ngọc, Bộ Nội vụ
9. Trương Mỹ Dung, ĐHKT TP HCM
10. F. Phạm, ĐH Nice, Pháp
11. M. Brodman, Zurich, Thụy Sỹ
12. Nhà Xuất bản Giáo dục
13. Nguyễn Đình Sang, ĐHQG HN
14. Viện Toán học, TTKHTN & CNQG
15. Ngô Việt Trung, Viện Toán học
16. Bùi Khắc Sơn, CĐSP Quảng Bình
17. Ngô Văn Lược, Vietsovpetro
18. Trung tâm KHTN & CNQG
19. Chương trình quốc gia NCCB về KHTN
20. Hoàng Tụy, Viện Toán học
21. Hà Huy Khoái, Viện Toán học
22. Nguyễn Tự Cường, Viện Toán học
23. Khoa Toán, ĐHSP Thái Nguyên
24. Phạm Ngọc Thao, ĐHQG HN
25. Masaaki YOSHIDA, Kyushu Univ., Nhật Bản
26. Đỗ Hồng Tân, Viện Toán học
27. Tạ Thị Hoài An, ĐHSP Vinh
28. Lê Thị Thanh Nhàn, ĐHSP Thái Nguyên
29. Lê Dũng Tráng, ĐH Marseille , Pháp
30. Phan Đình Diệu, ĐHQG HN
31. Khoa Toán-Tin, ĐHSP Vinh
32. Hoàng Mai Lê, CĐSP Thái Nguyên
33. ĐHKHTN, ĐHQG HN
34. Phan Quốc Khánh, ĐHQG TP HCM
35. Nguyễn Hữu Anh, ĐHQG TP HCM

36. Phan Huy Tỉnh, THPT Phan Bội Châu, Vinh, Nghệ An
37. Đinh Thị Xuân, CĐSP Thái Nguyên
38. Lê Tuấn Hoa, Viện Toán học
39. Ngô Bảo Châu, Univ. Paris 13, Pháp
40. Đinh Văn Huỳnh, Viện Toán học
41. CĐSP Quảng Bình
42. Lê Thị Hoài Thu, CĐSP Quảng Bình
43. Hoàng Đình Dung, Viện Toán học
44. Trần Tuấn Nam, Dự bị ĐH Nha Trang
45. Phạm Hữu Anh Ngọc, ĐHSP Huế
46. Trần Đình Long, ĐHSP Huế
47. Vũ Hoài An, CĐSP Hải Dương
48. Lê Ngọc Lăng, ĐH Mỏ-Địa chất HN
49. Nguyễn Ngọc Chu, Viện Toán học
50. Khoa Toán-Tin, ĐH Đà Lạt
51. Tạ Lê Lợi, ĐH Đà Lạt
52. Nguyễn Cam, ĐHSP TP HCM
53. Mỵ Vinh Quang, ĐHSP TP HCM
54. N. Koblitz, ĐH Washington, Mỹ
55. Nguyễn Chánh Tú, ĐHSP Huế
56. Trần Khánh Hưng, Nguyên cán bộ ĐHSP Huế
57. Uỷ ban nhân dân Tỉnh Hà Tĩnh
58. Uỷ ban nhân dân Tỉnh NGhệ An
59. Trần Văn Vuông, Viện KHGD
60. Trần Nam Dũng, ĐHQG TP HCM
61. Phạm Mạnh Tuyến, Sở GD ĐT Thái Nguyên
62. Lớp cao học khoá 10, Viện Toán học

Trong danh sách trên, có rất nhiều cơ quan và cá nhân đã ủng hộ nhiều lần.

Quỹ Lê Văn thiêm xin chân thành cám ơn các cá nhân và cơ quan đã nhiệt tình ủng hộ xây dựng Quỹ.

DANH SÁCH CÁC TIẾN SĨ TOÁN HỌC

bảo vệ trong nước đến tháng 9/2002 và đã được cấp bằng Tiến sĩ đến tháng 12/2002

TT	Họ và tên NCS Cơ quan công tác	Ngày bảo vệ Cơ sở đào tạo	Tên đề tài luận án Chuyên ngành	Người hướng dẫn khoa học
1.	Trịnh Đào Chiến Sở Giáo dục và Đào tạo Gia Lai	28/9/2001 ĐHKH TN Hà Nội	*Một số vấn đề về chuỗi Dirichlet suy rộng và ứng dụng* 1.01.01 — Toán giải tích	GS-TSKH Nguyễn Văn Mậu TS Lê Hải Khôi
2.	Đàm Văn Nhỉ CĐ SP Thái Bình	6/9/2001 Viện Toán học	*Đặc biệt hoá môđun hữu hạn sinh trên vành đa thức* 1.01.03 - Đại số và lý thuyết số	GS-TSKH Ngô Việt Trung PGS-TSKH Lê Tuấn Hoa
3.	Nguyễn Việt Hải ĐHSP Hải Phòng	12/9/2001 Viện Toán học	*Lượng tử hoá biến dạng trên các K-quỹ đạo và biểu diễn của hai nhóm MD và MD_4* 1.01.05 — Hình học và tôpô	GS-TSKH Đỗ Ngọc Diệp
4.	Hoàng Quang Tuyến	28/9/2001 Viện Toán	*Phương pháp tối ưu không lồi trên tập Pareto của bài*	PGS-TSKH Lê Dũng Mưu

	Sở KH, CN và MT Đà Nẵng	học	*toán đa mục tiêu phân tuyến tính* 1.01.09 — Vận trù học	TS Thái Quỳnh Phong
5.	Trần Minh Thuyết Trường đại học Kinh tế TP HCM	19/10/2001 ĐHSP TPHCM	*Định lí tồn tại và duy nhất nghiệm đối với một số bài toán biên phi tuyến* 1.01.01 — Toán giải tích	PGS-TS Trần Văn Tấn TS Trần Thành Long
6.	Vũ Hoài An CĐSP Hải Dương	13/11/2001 Viện Toán học	*Phân phối giá trị cho hàm và ánh xạ chỉnh hình p-adic nhiều biến* 1.01.03 - Đại số và lí thuyết số	GS-TSKH Hà Huy Khoái
7.	Trương Văn Thương ĐHSP - ĐH Huế	9/11/2001 Viện Toán học	*Một số tính chất của không gian Banach có chuẩn sinh bởi hàm lõm* 1.01.01 — Toán giải tích	GS-TSKH Trần Đức Vân PGS-TSKH Hà Huy Bảng
8.	Phạm Văn Thạo ĐH Ngoại ngữ - ĐHQGHN	20/12/2001 Viện Toán học	*Về khả năng biểu diễn ngôn ngữ của mạng Petri* 1.01.10 - Đảm bảo toán học cho MT và HTTT	PGS-TS Phạm Trà Ân TS Kiều Đức Thành
9.	Vũ Thị Thái CĐSP Thái Nguyên	23/11/2001 ĐH Sư phạm Hà Nội	*Bước đầu hình thành và phát triển trí tưởng tượng không gian cho học sinh tiểu học thông qua dạy học các yếu tố hình học* 5.07.02 — Phương pháp giảng dạy toán	PGS-TS Trần Thúc Trình
10.	Nguyễn Bá Minh ĐH Thương mại Hà Nội	31/12/2001 Viện Toán học	*Một số tính chất của ánh xạ đa trị và ứng dụng của chúng trong lí thuyết tối ưu vectơ đa trị* 1.01.09 — Vận trù học	PGS-TSKH Nguyễn Xuân Tấn. TS Vũ Văn Đạt
11.	Đinh Tấn Phước Cục Hàng không Dân dụng VN	7/9/2001 ĐH Vinh	*Góp phần hoàn thiện nội dung và phương pháp dạy học các yếu tố hình học giải tích cho các lớp chuyên toán ở bậc trung học của VN* 5.07.02 — PPGD Toán	PGS-TS Đào Tam
12.	Nguyễn Mạnh Chung ĐH Hồng Đức, Thanh Hóa	14/12/2001 Viện Khoa học giáo dục	*Nâng cao hiệu quả dạy khái niệm toán học bằng các biện pháp sư phạm theo hướng tích cực hoá hoạt động nhận thức của học sinh* 5.07.02 — PPGD Toán	PGS-TS Ngô Hữu Dũng TS Nguyễn Hữu Châu
13.	Nguyễn Sỹ Đức Sở Giáo dục và Đào tạo Hoà Bình	20/5/2002 ĐHSP Hà Nội	*Xây dựng và sử dụng phần mềm dạy học hỗ trợ luyện tập môn toán ở trường tiểu học*	GS-TSKH Nguyễn Bá Kim TS Nguyễn Thái Lai

			5.07.02 — PP GD Toán	Lai
14.	Hồ Cẩm Hà ĐHSP Hà Nội	18/5/2002 ĐH Bách khoa Hà Nội	*Một cách tiếp cận mở rộng cơ sở dữ liệu quan hệ với thông tin không đầy đủ* 1.01.10 - Đảm bảo toán học cho MT và HTTT	PGS-TS Hồ Thuần TS Nguyễn Thanh Thuỷ
15.	Phan Văn Thiện ĐHSP - Đại học Huế	28/6/2002 Viện Toán học	*Chặn trên Serge cho chỉ số chính quy của tập điểm béo trong không gian xạ ảnh* 1.01.03 - Đại số và lý thuyết số	GS-TSKH Ngô Việt Trung PGS-TSKH Lê Tuấn Hoa
16.	Đặng Quang Việt Trường đại học Tây Bắc	16/7/2002 Viện Khoa học giáo dục	*Tăng cường định hướng sư phạm trong dạy học Đại số đại cương thông qua việc xây dựng một số chuyên đề cho sinh viên toán cao đẳng sư phạm* 5.07.02 — PPGD Toán	PGS-TS Nguyễn Hữu Châu PGS-TSKH Đỗ Đức Thái
17.	Nguyễn Thị Tuyết Mai ĐHSP Thái Nguyên	3/9/2002 ĐHSP Hà Nội	*Một số định lí về ánh xạ chỉnh hình tách biến và thác triển chỉnh hình kiểu Noguchi* 1.01.01 — Toán giải tích	PGS-TSKH Đỗ Đức Thái TS Khu Quốc Anh

TIN TỨC HỘI VIÊN VÀ HOẠT ĐỘNG TOÁN HỌC

LTS: *Để tăng cường sự hiểu biết lẫn nhau trong cộng đồng các nhà toán học Việt Nam, Toà soạn mong nhận được nhiều thông tin từ các hội viên HTHVN về chính bản thân mình, cơ quan mình hoặc đồng nghiệp của mình.*

Hội thảo khoa học

Nhân dịp đầu Xuân Quí Mùi, **Hội thảo khoa học: Chương trình giảng dạy Toán học ở đại học và trên đại học** do Hội Toán học chủ trì đã được tổ chức tại Thác Đa, một địa điểm nghỉ mát ở chân núi Ba Vì. Kết hợp với Hội thảo là buổi gặp mặt truyền thống các thế hệ toán học trong và gần Hà Nội nhân dịp đầu xuân.

Tới dự Hội thảo có hơn 160 cán bộ, chủ yếu của các cơ quan tại Hà Nội. Một số đơn vị xa như ĐH Vinh, ĐH Thái Nguyên, ... biết tin cũng đa dăng kí tham dự. Nhiều ý kiến tranh luận sôi nổi đã diễn ra. Đa số ý kiến cho rằng năm 2003 cần tổ chức một hội nghị khoa học qui mô hơn bàn về vấn đề này.

Kết thúc Hội thảo là buổi gặp mặt truyền thống và Lễ trao Giải thưởng Lê Văn Thiêm cho một thầy giáo và 4 học sinh có thành tích xuất sắc trong năm 2002.

Chúc thọ

Nhân dịp GS Ngô Thúc Lanh 80 tuổi, Khoa Toán, ĐHSP Hà Nội đã tổ chức Lễ mừng thượng thọ vào ngày 22/2/2003. Hội Toán học xin chúc mừng Giáo sư, và kính chúc Giáo sư và gia đình mạnh khỏe, hạnh phúc.

Trách nhiệm mới

1. PGS-TS Ngô Sỹ Tùng được bổ nhiệm giữ chức vụ Trưởng khoa Toán, trường Đại học Vinh từ tháng 12/2002. Anh sinh ngày 01/9/1957 tại Bắc Thành, Yên Thành, Nghệ An. Anh tốt nghiệp khoa Toán Đại học Sư phạm Vinh năm 1977 và bảo vệ luận án Tiến sĩ năm 1995. Năm 2002 được Nhà nước phong học hàm Phó giáo sư. Giữ chức vụ Phó trưởng khoa Toán từ tháng 10/1998 đến tháng 12/2002.

2. TS Phạm Ngọc Bội được bổ nhiệm giữ chức vụ Phó trưởng khoa Toán trường Đại học Vinh từ tháng 12/2002. Anh sinh ngày 16/12/1954 tại Hải Hậu, Nam Định. Anh tốt nghiệp Khoa Toán trường Đại học Sư phạm Vinh năm 1976 và bảo vệ luận án Tiến sĩ năm 2001.

3. TS Nguyễn Thành Quang được bổ nhiệm giữ chức vụ Phó trưởng khoa Toán trường Đại học Vinh từ tháng 12/2002. Anh sinh ngày 18/3/1958 tại Thành phố Vinh, Nghệ An. Anh tốt nghiệp Khoa Toán trường Đại học Sư phạm Vinh năm 1979 và bảo vệ luận án Tiến sĩ năm 1998.

Đại học Thái Nguyên vừa thành lập Khoa khoa học tự nhiên trực thuộc trường. Sau đây là những cán bộ chủ chốt của khoa:

4. TS Nông Quốc Chinh được bổ nhiệm chức vụ Trưởng khoa từ tháng 10/2002. Anh sinh năm 1956 tại Cao Bằng. Tốt nghiệp ĐHSP Việt Bắc năm 1977, bảo vệ luận án tiến sĩ về Đại số năm 1995 tại Tiệp Khắc. Là chủ nhiệm Khoa Toán ĐHSP Thái Nguyên từ 1997-2001, trưởng phòng đào tạo ĐHSP Thái Nguyên từ tháng 1 đến tháng 10/2002.

5. ThS. Nguyễn Đức Lạng được bổ nhiệm chức vụ Trưởng phòng tổng hợp của Khoa từ tháng 10/2002. Anh sinh năm 1959 tại Lạng Sơn. Tốt nghiệp ĐHSP Việt Bắc năm 1978, và bảo vệ luận văn thạc sĩ về Toán năm 1996, thạc sĩ về Tin năm 1999.

6. TS Lê Thị Thanh Nhàn được bổ nhiệm chức vụ Trưởng phòng đào tạo của Khoa từ tháng 10/2002. Chị sinh năm 1970. Tốt nghiệp ĐHSP Việt Bắc năm 1990, bảo vệ luận án tiến sĩ về Đại số năm 2001 tại Viện Toán học.

Đầu năm 2002, ĐH Thái Nguyên cũng đã thành lập Khoa Công nghệ Thông tin trực thuộc. Sau đây là một số cán bộ toán giữ trách nhiệm quản lí.

7. ThS. Vũ Mạnh Xuân được bổ nhiệm chức vụ Phó trưởng khoa Công nghệ Thông Tin, ĐH Thái Nguyên từ tháng 3/2002. Anh sinh năm 1956 tại Vĩnh Phúc. Tốt nghiệp ĐHSP Việt Bắc năm 1977, tốt nghiệp cao học về Toán năm 1979, bảo vệ luận văn thạc sĩ Tin học năm 1999. Là Phó chủ nhiệm Khoa Toán ĐHSP Thái Nguyên từ 1997-2001.

8. ThS. Vũ Vinh Quang được bổ nhiệm chức vụ Trưởng phòng tổng hợp khoa Công nghệ Thông Tin, ĐH Thái Nguyên từ tháng 3/2002. Anh sinh năm 1957 tại Thái Nguyên. Tốt

nghiệp ĐHTH Hà Nội năm 1978, bảo vệ luận văn thạc sĩ Tin học năm 1999.

Đính chính: Do sơ suất, Trong các số 2 Tập 1(1997), tr. 12 và số 4 Tập 6(2002), tr. 14 Thông tin Toán học đã đưa sai tin tức về GS Hoàng Tụy. Giáo sư sinh năm 1927, và không theo học lớp Toán đại cương do GS Nguyễn Thúc Hào dạy ở Khu 4 cũ, năm 1947. Ban biên tập thành thật xin lỗi GS Hoàng Tụy và quí vị độc giả.

GIẢI THƯỞNG KHOA HỌC VIỆN TOÁN HỌC 2003

Như thông báo đã đưa trong THÔNG TIN TOÁN HọC Tập 1 Số 2 (1997), tr. 10, Giải thưởng khoa học Viện toán học được trao 2 năm một lần, *vào các năm lẻ*. Chúng tôi xin nhắc lại ở đây những **nội dung chính**:

1. Mọi cán bộ nghiên cứu và giảng dạy toán học của Việt Nam, tuổi đời không quá 40 (sinh từ năm 1963 trở về sau) đều có quyền đăng kí xét thưởng.
2. Người được Giải thưởng sẽ được nhận một Giấy chứng nhận và 5.000.000 VNĐ.

Hồ sơ đăng kí xét thưởng gồm:

1. Lí lịch khoa học.
2. Danh mục công trình nghiên cứu đã công bố.
3. Một số (không quá 5) công trình tiêu biểu.
4. Một bản giới thiệu thành tích nghiên cứu khoa học của người đăng kí (do đơn vị công tác của người đó viết)

Lịch xét Giải thưởng khoa học Viện Toán học 2003:

1. Hạn nhận hồ sơ: đến hết ngày 30/9/2003.
2. Giải thưởng sẽ được công bố vào 30/11/2003.

Những người đã đăng kí tham dự Giải thưởng vào các năm trước nhưng chưa được trao giải thưởng, nếu sinh từ năm 1963 trở về sau, vẫn có thể đăng kí tham dự Giải thưởng 2003. Trong trường hợp đó, người đăng kí chỉ cần gửi thư khẳng định nguyện vọng đăng kí tham dự Giải thưởng 2003 và những thông tin mới nhất (nếu có) về kết quả nghiên cứu.

Hồ sơ xin gửi về địa chỉ

Ngô Việt Trung
Viện Toán học
Hộp thư 631 Bờ Hồ Hà Nội
Fax: (04)8343303
E-mail: nvtrung@thevinh.ncst.ac.vn

Kính mời quí vị và các bạn đồng nghiệp
đăng kí tham gia Hội Toán Học Việt Nam

Hội Toán học Việt Nam được thành lập từ năm 1966. Mục đích của Hội là góp phần đẩy mạnh công tác giảng dạy, nghiên cứu phổ biến và ứng dụng toán học. Tất cả những ai có tham gia giảng dạy, nghiên cứu phổ biến và ứng dụng toán học đều có thể gia nhập Hội. Là hội viên, quí vị sẽ được phát miễn phí tạp chí Thông Tin Toán Học, được mua một số ấn phẩm toán với giá ưu đãi, được giảm hội nghị phí những hội nghị Hội tham gia tổ chức, được tham gia cũng như được thông báo đầy đủ về các hoạt động của Hội. Để gia nhập Hội lần đầu tiên hoặc để dăng kí lại hội viên (theo từng năm), quí vị chỉ việc điền và cắt gửi phiếu đăng kí dưới đây tới BCH Hội theo địa chỉ:

Chị Khổng Phương Thúy, Viện Toán Học, Hộp thư 631, Bưu điện Bờ Hồ, Hà Nội.

Về việc đóng hội phí có thể chọn một trong 4 hình thức sau đây:

1. Đóng tập thể theo cơ quan (kèm theo danh sách hội viên).
2. Đóng trực tiếp cho một trong các đại diện sau đây của BCH Hội tại cơ sở:

Hà Nội: ô. Nguyễn Duy Tiến (ĐHKHTN); c. Khổng Phương Thúy (Viện Toán Học); ô. Doãn Tam Hòe (ĐH Xây dựng); ô. Phạm Thế Long (ĐHKT Lê Quý Đôn); ô. Tống Đình Quì (ĐH Bách khoa); ô. Vũ Viết Sử (ĐH Sư phạm 2)

Các thành phố khác: ô. Trần Ngọc Giao (ĐHSP Vinh); ô. Phạm Xuân Tiêu (CĐSP Nghệ An); ô. Lê Viết Ngư (ĐH Huế); bà Trương Mỹ Dung (ĐHKT Tp HCM); ô. Nguyễn Bích Huy (ĐHSP Tp HCM); ô. Nguyễn Hữu Anh (ĐHKHTN Tp HCM); ô. Nguyễn Hữu Đức (ĐH Đà Lạt); ô. Đặng Văn Thuận (ĐH Cần Thơ).

3. Gửi tiền qua bưu điện đến cô Khổng Phương Thúy theo địa chỉ trên.
4. Đóng bằng tem thư (loại tem không quá 1000Đ, gửi cùng phiếu đăng kí).

BCH Hội Toán Học Việt Nam

Hội Toán Học Việt Nam
PHIẾU ĐĂNG KÍ HỘI VIÊN

1. Họ và tên:

Khi đăng kí lại quí vị chỉ cần điền ở những mục có thay đổi trong khung màu đen này

2. Nam ☐ Nữ ☐
3. Ngày sinh:
4. Nơi sinh (huyện, tỉnh):
5. Học vị (*năm, nơi bảo vệ*):
   Cử nhân:
   Ths:
   TS:
   TSKH:
6. Học hàm (*năm được phong*):
   PGS:
   GS:
7. Chuyên ngành:
8. Nơi công tác:
9. Chức vụ hiện nay:
10. Địa chỉ liên hệ:

E-mail:
ĐT:

Ngày: Kí tên:

Hội phí năm 2003

Hội phí : 20 000 Đ ☐

Acta Math. Vietnam. 70 000 Đ ☐

Tổng cộng:

Hình thức đóng:

☐ Đóng tập thể theo cơ quan (tên cơ quan):

☐ Đóng cho đại diện cơ sở (tên đại diện):

☐ Gửi bưu điện (xin gửi kèm bản chụp thư chuyển tiền)

☐ Đóng bằng tem thư (gửi kèm theo)

Ghi chú: - Việc mua Acta Mathematica Vietnamica là tự nguyện và trên đây là giá ưu đãi (chỉ bằng 50% giá chính thức) cho hội viên (gồm 3 số, kể cả bưu phí).

- Gạch chéo ô tương ứng.

Mục lục